



Australian Government
Department of Defence
Defence Science and
Technology Organisation

A Review of the Capability Options Development and Analysis System and the Role of Risk Management

Svetoslav Gaidow¹, Seng Boey² and Richard Egudo¹

¹Land Operations Division

²Air Operations Division

Defence Science and Technology Organisation

DSTO-GD-0473

ABSTRACT

Capability development is a complex process that requires significant science & technology support and a rigorous analytical background. In the Australian Army, this need has led to the design of the Capability Options Development and Analysis System (CODAS) at the Force Development Group of the Land Warfare Development Centre. This document contributes towards analysis of CODAS as a system, the evolution of its architecture and its role as an analytical support framework for capability development in the Army. It also aims to reveal the potential of risk management as a valuable analysis and decision-making support tool belonging to CODAS. The application of risk management in capability development can be viewed as realisation of the CODAS methodology and thus raises the profile of CODAS in the Army Continuous Modernisation Process.

RELEASE LIMITATION

Approved for public release

Published by

*Land Operations Division
DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia*

Telephone: (08) 8259 5555

Fax: (08) 8259 6567

*© Commonwealth of Australia 2006
AR 013-727*

Submitted: February 2005

Published: August 2006

APPROVED FOR PUBLIC RELEASE

A Review of the Capability Options Development and Analysis System and the Role of Risk Management

Executive Summary

The Australian Army must be able to provide land forces ready to meet the demands of current high-level guidance, influence the regional international relations, and be able to respond quickly to changes in technology and the strategic environment. The Army Continuous Modernisation Process (ACMP) is the means used to establish future force options and to coordinate Army's capability development efforts. Capability development is a complex process, which requires a systematic approach featuring a rigorous analytical background and a significant science and technology support. In response to this need, the Capability Options Development and Analysis System (CODAS) was developed at the Force Development Group of the Land Warfare Development Centre. CODAS is an evolving system; and recently endorsed concepts and major reviews in Defence, such as *Force 2020*, *Future Warfighting Concept* and the *Defence Procurement Review 2003* had a significant impact on CODAS and led to changes in CODAS as a concept and construct.

CODAS can link strategic guidance and future force options, identify capability gaps and deficiencies, develop and compare capability options, and produce migration paths between current and future capabilities. CODAS possesses the methodological support necessary for performing the various activities within the ACMP, and has become an inherent part of the process. Army has already employed CODAS to produce future land force options such as the set of Objective Force papers and the Hardened and Networked Army (HNA) model. Moreover, the HNA was endorsed by the Australian Government and there is a plan for its implementation in the period 2006 – 2015. This has shown that CODAS can work and provide support to developers and decision makers in Army.

By design, CODAS possesses an analytical subsystem that supports assessment, evaluation and validation of force options and associated development plans – the Capability Development and Evaluation Toolset. The toolset features a broad variety of approaches and techniques covering areas such as optimisation, simulation, modelling, forecasting, systems engineering, experimentation, wargaming and risk management. Examples of risk management applications into capability development, have given a clear indication of the potential of risk management. The risk analysis studies of the rotation model in Land Command 2003 and the HNA are illustrative examples of risk management in action. Risk management has emerged as a valuable decision-making support tool in CODAS. Moreover, the applications of risk management discussed in this document can be viewed as a successful application of the CODAS methodology and can serve as confirmation of the importance of CODAS to the process of continuous modernisation in Army.

Contents

1. INTRODUCTION	1
2. ARMY CAPABILITY DEVELOPMENT.....	3
2.1 Capability Systems in Defence	3
2.2 Army Continuous Modernisation Process	5
2.3 Coherent Force Development: A Review of ACMP	8
2.4 Defence Procurement Review (DPR 2003)	10
2.5 Army Science and Technology Requirements and Priorities	14
3. CAPABILITY OPTIONS DEVELOPMENT & ANALYSIS SYSTEM (CODAS) ..	16
3.1 CODAS Fundamentals	17
3.2 CODAS Architecture.....	18
3.3 CODAS Processes	23
3.4 Capability Development and Evaluation Toolset	25
3.5 CODAS Implementation and Further Development.....	27
4. APPLICATIONS OF RISK MANAGEMENT.....	29
4.1 Capability Development Analyses.....	29
4.2 Risk Management Implications from DPR 2003	31
4.3 Force Structure and Force Preparedness.....	32
4.4 Force Option Testing.....	33
4.5 Hardened and Networked Army	35
5. CONCLUDING REMARKS.....	39
6. ACKNOWLEDGEMENTS.....	40
7. REFERENCES.....	40
APPENDIX A: FUNDAMENTAL INPUTS TO CAPABILITY	45
APPENDIX B: RISK MANAGEMENT IN DEFENCE	47
B.1. Australian Defence Risk Management Framework	47
B.2. Summary of the Risk Management Process.....	49

Figures

Figure 1: Fundamental Inputs to Capability (from [7])	3
Figure 2: Capability Systems Life Cycle (from [7]).....	4
Figure 3: Army Development Continuum (from ACMP [1])	6
Figure 4: Capability Systems Life Cycle (Post-Kinnaird) (from DPR 2003 [11])	11
Figure 5: Technology Readiness Levels (from DPR 2003 [11])	14
Figure 6: S&T Support for Army CSLC Process (from ASTRAP 05 [12]).....	15
Figure 7: Army Capability Management (from ACMP 2001-2005 [8])	16
Figure 8: CODAS in relation to AEF and ACMP (from [2])	17
Figure 9: Description of CODAS as a System (from [2]).....	19
Figure 10: Systems Architecture Supporting CODAS (from [2]).....	20
Figure 11: Achieving Effects = Applying Capabilities to perform Functions to realise Objectives (from [21]).....	21
Figure 12: Effects (from [21]).....	22
Figure 13: Capability Options Analyses (from [3]).....	25
Figure 14: Capability Analyses and Risk Management (from [29])	30
Figure 15: Applicability in Defence Capability (from [29])	32
Figure 16: Summary of FOT: Method and Measures (from [34])	34
Figure 17: Land force evolutionary planning process.....	35
Figure 18: Example of ranked differences (medium risks) between AIB+ and HNA	37
Figure 19: Summary of major differences between AIB+ and HNA	38
Figure 20: HNA is better network enabled.....	39
Figure 21: Australian Defence Risk Management Framework.....	47
Figure 22: Managing Risks in Defence (adapted from DRM Implementation Plan [47])	48
Figure 23: Risk Management Process (from AS/NZS 4360:2004 [36]).....	50
Table 1: Qualitative Measures of Consequence/Impact (from HB 436:2004 [49])	53
Table 2: Qualitative Measures of Likelihood (from HB 436:2004 [49])	53
Table 3: Qualitative Risk Analysis Matrix (from HB 436:2004 [49]).....	53
Figure 24: Risk/Opportunity Matrix (from [50])	54
Figure 25: ALARP Principle (from [49])	55

Tables

Table 1: Qualitative Measures of Consequence/Impact (from HB 436:2004 [49])	53
Table 2: Qualitative Measures of Likelihood (from HB 436:2004 [49])	53
Table 3: Qualitative Risk Analysis Matrix (from HB 436:2004 [49]).....	53

Glossary

AAN	Army After Next
ABCA	America, Britain, Canada and Australia
ABD	agent based distillation
ACMP	Army Continuous Modernisation Process
ACR	Army Capability Requirement
ADF	Australian defence Force
ADO	Australian Defence Organisation
AEF	Army Experimental Framework
AHP	Analytic Hierarchy Process
AIB	Army In Being
AIPS	Australian Illustrative Planning Scenarios
ALARP	as low as reasonably practicable
APCOD	Army Preliminary Capability Options Document
AS/NZS	Australian Standard/New Zealand Standard
ASTORP	Australian Theatre Operational Preparedness Requirement
ASTRAP	Army Science & Technology Requirements and Priorities
BOS	Battlespace Operational System
CADI	Chief of Army's Development Intent
CASAC	Chief of Army's Senior Advisory Committee
CDET	Capability Development and Evaluation Tool
CDF	Chief of the Defence Force
CDS	Chief Defence Scientist
CED	Concept for Employment Document
CEI	Chief Executive's Instruction
CODAS	Capability Options Development and Analysis System
CPD	Chief of Defence Force Preparedness Directive
CSIRO	Commonwealth Scientific & Industrial Research Organisation
CSLC	Capability Systems Life Cycle
CSLCMM	Capability Systems Life Cycle Management Manual
DCDM	Defence Capability Development Manual
DCP	Defence Capability Plan
DCPG	Defence Capability Planning Guidance
DERM	Defence Enterprise Risk Management
DFGW	Direct fire guided weapon
DGFLW	Director General Future Land Warfare
DLOC	Directed Level of Capability
DMO	Defence Materiel Organisation
DOORS	Dynamic Object Oriented Requirements System
DPR	Defence Procurement Review
DRMF	(Australian) Defence Risk Management Framework
DRMIP	Defence Risk Management Implementation Plan
DRMP	Defence Risk Management Policy
DRN	Defence Restricted Network
DSTO	Defence Science and Technology Organisation
FDG	Force Development Group
FE	Force Element
FEG	Force Element Group
FIC	Fundamental Input to Capability

FLW	Future Land Warfare
FOT	Force Options Testing
FRA	Force Research Area
FRAC	Force Research Area Capability
FYMCEP	Five-Year Minor Capital Equipment Program
HNA	Hardened and Networked Army
IBC	Initial Business Case
KFOC	key function of capability
LWDC	Land Warfare Development Centre
MOLE	Manoeuvre Operations in a Littoral Environment
ODP	Output Development Plan
OF	Objective Force
SME	Subject Matter Expertise
S&T	Science & Technology
SWOT	strengths, weaknesses, opportunities and threats
TARDIS	The ADF Requirements Development Information System
T&E	test and evaluation
TRL	Technology Readiness Level
TTCP	The Technical Cooperation Program
UK	United Kingdom
US	United States (of America)
VCDF	Vice Chief of the Defence Force

1. Introduction

The Australian Army is committed to the path of continuous modernisation, which enables Government to possess capabilities that guarantee *the security of Australia and protect its people and interests both now and in the future* [1]. The Army must be able to provide land forces ready to meet the demands of current high-level guidance, influence the regional international relations, and be able to respond quickly to changes in technology and the strategic environment. The Army Continuous Modernisation Process (ACMP) is the means used to establish future options and to coordinate Army's capability development efforts necessary to achieve its desired warfighting outcomes. The ACMP provides a concept-led and capability-based framework for Army's modernisation. However, capability development is a complex process, which requires a systematic approach featuring a rigorous analytical background and adequate science & technology support.

In response to this need, the Capability Options Development and Analysis System (CODAS) was designed at the Force Development Group of the Australian Army's Land Warfare Development Centre. For details refer to [2]. CODAS has been developed to support the process of capability development in Army and hence possess the capacity to perform a wide range of activities including:

- Establish the linkage between strategic guidance and future force options;
- Design, test and evaluate future force options;
- Compare competing capability options;
- Develop migration paths between current and future capabilities;
- Identify capability gaps and deficiencies, high pay-off areas and contentious issues, etc.

This document focuses on the structure and attributes of CODAS and follows the various modifications in the evolution of the system as a concept and as a construct. It investigates the potential of CODAS to function successfully, and ultimately whether CODAS contains the methodological support needed to make the ACMP work. The review takes into account a number of published and unpublished documents and presentations by various participants in the development of CODAS — see for example [3], [4] and [5],.

The recent endorsement of the enterprise risk management approach in Defence paved the way for the establishment of an entirely different risk management culture in Defence, where all personnel have to implement risk management in any activity they participate in. Thus, the capability development process also has to be aligned with, and based on this risk management approach. Indeed, the Foreword of the Defence Capability Development Manual (DCDM) [6] requests that *the areas of risk and degrees of risks are properly identified and managed*. However, neither DCDM nor the Capability Systems Life Cycle Management Manual (CSLCMM) [7] reflect the new trend in applying risk management to discover opportunities, that is, to look for what can be improved.

This document also focuses on risk management as one of the components of the Capability Development and Evaluation Toolset (CDET) of CODAS. The analytical

nature of risk management and its complementarity in relation to many other methods determines its good fit into the CDET. CODAS provides a suitable framework for demonstrating the potential of risk management. On the other hand, the successful employment of risk management in capability development would increase the profile of CODAS as the analytical support framework for ACMP.

This document begins by describing the context of capability development in Army. First, the capability system life cycle model is considered, which forms the foundation for capability management in Defence and in Army, for details refer to [6] and [7]. Second, the current ACMP is introduced [1] and references are made to its previous versions [8] and [9]. The Review [10] of the ACMP from 2003 is discussed next, followed by a brief summary of the Defence Procurement Review 2003 [11] and the Army Science and Technology Requirements and Priorities 2005-08 [12]. The Kinnaird Review [11] marks a big change with the recommendation to introduce a mandatory technical risk assessment for each project. For DSTO in particular, this means a greatly increased role and responsibility as the authority for technical risk in Defence. The detailed description of these major elements in the process of Army's capability modernisation establishes the broad background for emphasising the role of CODAS, and specifically the potential of risk management in capability development.

This publication focuses on activities conducted, documents published and events observed in the period early 2002 to early 2005. It does not cover any recent events, which may be the target of another investigation. The document provides a description of the original design of CODAS and the enhancements made later, which have influenced its continuing evolution as a concept, its structure and potential. The development of a force allocation model and tool and the application of agent based distillations are examples of the recent evolution of CODAS. Particular attention is paid to CDET containing a broad variety of methods and techniques including risk management. The document continues with an overview of actual and potential contributions of risk management to defence and particularly army capability development. A discussion is conducted of the applicability of risk management in capability development, in force structure and preparedness, and in force option testing. Examples of successful implementation of risk management are provided. The contribution of risk management to the Hardened and Networked Army is discussed in some detail. Finally, concluding remarks highlight the importance of applying CODAS and risk management in capability development and identify areas for future research. For completeness, this document contains two appendices: a summary of the Fundamental Inputs to Capability and a summary of the risk management process as adopted in the Department of Defence. They are provided mainly for reference.

2. Army Capability Development

2.1 Capability Systems in Defence

A capability usually means *the capacity to be or do or affect something*, i.e. it can refer to a *quality, capacity or ability* [6]. However, in Defence a *capability* has a more specific meaning and is formally defined as the *power to achieve a particular operational effect in a nominated environment at a given time and to sustain that effect for a designated period* [6], [7] *. Any capability is delivered by a system or systems which possess one or more of the Fundamental Inputs to Capability (FIC) as shown by Figure 1. The set of FICs established in Defence consists of: collective training, command and management, facilities, major systems, organisation, personnel, supplies, and support. Appendix A contains the detailed descriptions of the FICs as endorsed by the Deputy Secretary of Defence, Strategy, in June 2001.

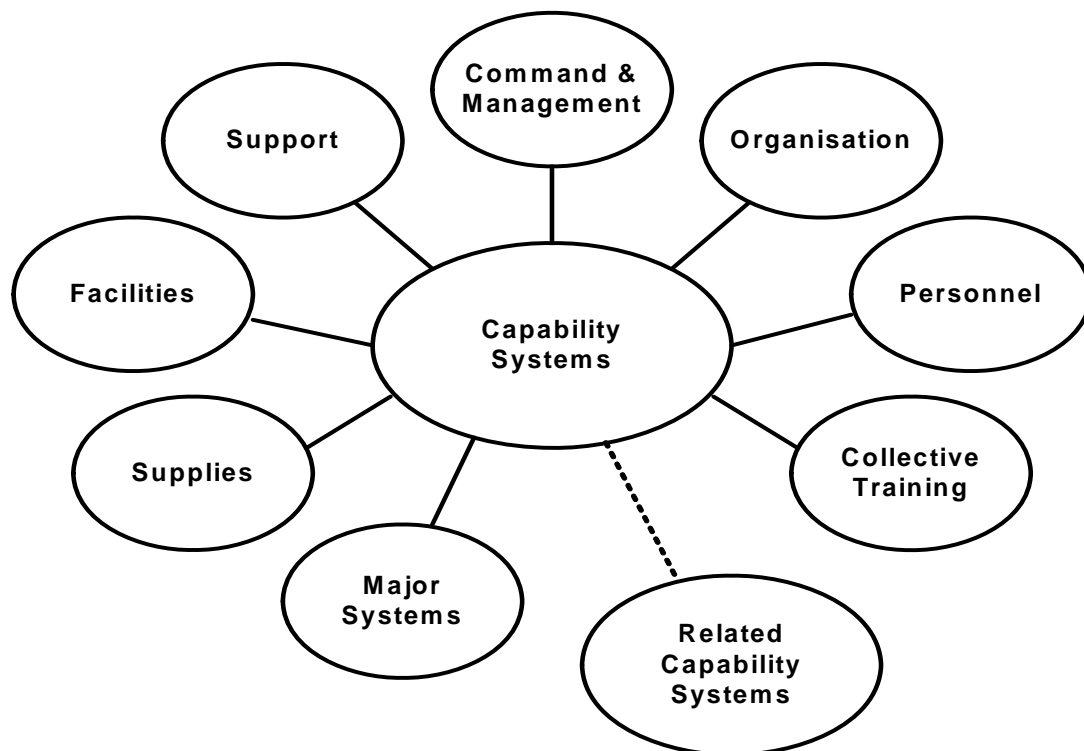


Figure 1: Fundamental Inputs to Capability (from [7])

FICs work together to generate capability and hence achieve desired effects. However, each of the inputs may have impact on the performance of the system(s) as a whole. Inevitably, a particular capability system also interacts with other capability systems in

* The second edition of the *Defence Capability Development Manual* [6], released in February 2006 is the current primary source of guidance regarding the capability development in the Australian Defence Organisation. It covers the first two phases of the capability life cycle – need and requirements, while the *Capability Systems Life Cycle Management Manual* [7] covers all five of them, see also Figure 2. However, publication [6] discusses the requirements phase, and the recently introduced first pass approval and second pass approval in detail.

its external environment. Thus, following a holistic way of thinking, the focus is on the capability system as a connected whole and not as a set of discrete elements.

Capability systems have life cycles, which *begin with the identification of the need to reduce a current or prospective capability gap* [6]. This need is then step by step translated into a working system, which is operated and supported until it is withdrawn from service and disposed of. Every capability system life cycle consists of the following phases: identification of need, requirements, acquisition, in service, and disposal as shown by Figure 2. An overview of the life cycle for capability systems in Defence is provided in Section 1.1 of [6]. It shows also the organisational arrangements in the life cycle management process.

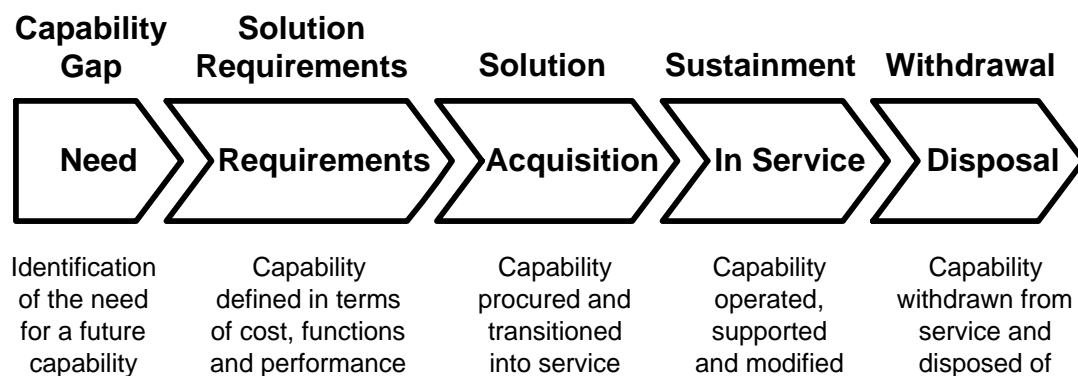


Figure 2: Capability Systems Life Cycle (from [7])

Thus, any defence capability is managed from system and life cycle perspectives. According to [6], the key management objectives are as follows:

- The development of the capability system must be optimised to address the gap(s), meet the requirements and manage the associated risks.
- The management of the capability system must be optimised with respect to its entire life cycle costs.
- The life cycles of various capability systems must be *orchestrated so that collectively they optimise the ability of Defence to carry out its missions and roles.*

Furthermore, the capability development process is based on broad strategic guidance, which is approved by Government in Defence White Papers and Annual Strategic Reviews, or is more specifically formulated in Australia's Military Strategy, Australian Illustrative Planning Scenarios (AIPS), operational concepts and military experimentation. However, the high-level capability planning is documented in the Defence Planning Guidance, the Defence Capability Strategy and the Defence Capability Plan. The aim is to examine the performance of current capabilities and the future capability needs within the 'big picture' of strategic circumstances and finite resources. Here, the challenge is in linking strategy, objectives, plans, budgets and performance measures, which includes:

- linking strategic guidance and capability planning, which consists of:
 - exhibiting the links between Government and Defence strategic guidance and the planning and resourcing of capability development in Defence,

- highlighting the synergies and links between and within major capabilities,
- contributing to the annual review of the Defence Capability Plan;
- facilitating prioritisation of capability development initiatives, which includes:
 - describing the overall capabilities in Defence; translating strategic guidance into planning guidance to better describe required capabilities,
 - providing guidance for the prioritisation of capability options;
- providing capability developers with guidance in regard to:
 - identifying and reporting capability gaps,
 - providing recommendations on required capabilities without giving solutions.

The recently established Capability Development Group plays a leading role in the life cycle management of capability systems in Defence. Its responsibilities include capability definition and contribution to the management of major capital investment programs. It develops *capability proposals consistent with strategic priorities and funding guidance for consideration and approval by Government* [6]. However, the life cycle management responsibilities are usually spread across groups in Defence. Specifically, the single services play an important contributing role, sometimes a primary role in the capability management process. For example, the Chief of Army is in charge of all in-service capabilities required to ‘win the land battle’.

2.2 Army Continuous Modernisation Process

Army’s ability to fulfil its mission depends upon how successfully it remains a potent, versatile, flexible and agile force able to contribute to the Australian Defence Force and the security of Australia. Army must continually modernise in terms of military thinking and technological development. The Army Continuous Modernisation Process (ACMP) [1] describes and coordinates Army’s capability development process and staff effort. It establishes what actions are required to identify, select and develop Army’s capabilities. ACMP specifies the duties of the different agencies in modernising the Army. It aligns the Army’s modernisation to the capability systems life cycle in Defence. ACMP covers all phases of the CSLC and follows a concept-led capability-based approach. It has ceased to be just a plan [8] and has evolved into a process; for details refer to [9] and then [1].

ACMP provides the framework for a concept-led and capability-based approach to Army’s modernisation. Future strategic requirements, technologies and warfighting concepts are taken into consideration and are matched with extant and/or already programmed capabilities. Moreover, future land force capability needs are discussed on the basis of required operational effects. The approach appears to target broad concepts rather than specific solutions. Hence, the Army can be in the position of exploring ways to meet its strategic requirements in rapidly changing circumstances. This approach also aims to allow the Army to better guide the development of military capabilities within a joint and coalition environment. The future warfighting concepts identify how the Army wishes to fight, and provide a framework for the convergence of force development with FICs management.

Capability development in the Army is led by concepts via the Army Development Continuum. It links together the present land force with future land force structures through backcasting as depicted for example in Figure 3. Here Army in Being (AIB) stands for the Army of today, Objective Force (OF) is a 20-year projection into the future

and Army after Next (AAN) focuses on a 30-year timeframe*. Backcasting is expected to have a major impact on the design of the OF based on emerging new warfighting concepts and technologies from AAN studies. Similarly, the OF design may be backcast to the AIB in order to identify opportunities for rapid enhancement of the present force. Backcasting has to be conducted on a continual basis so that new ideas, concepts and technologies are constantly identified, evaluated as appropriate to Army's requirements, and accepted for realisation. Thus it allows existing force structure models to evolve towards future force structure models.

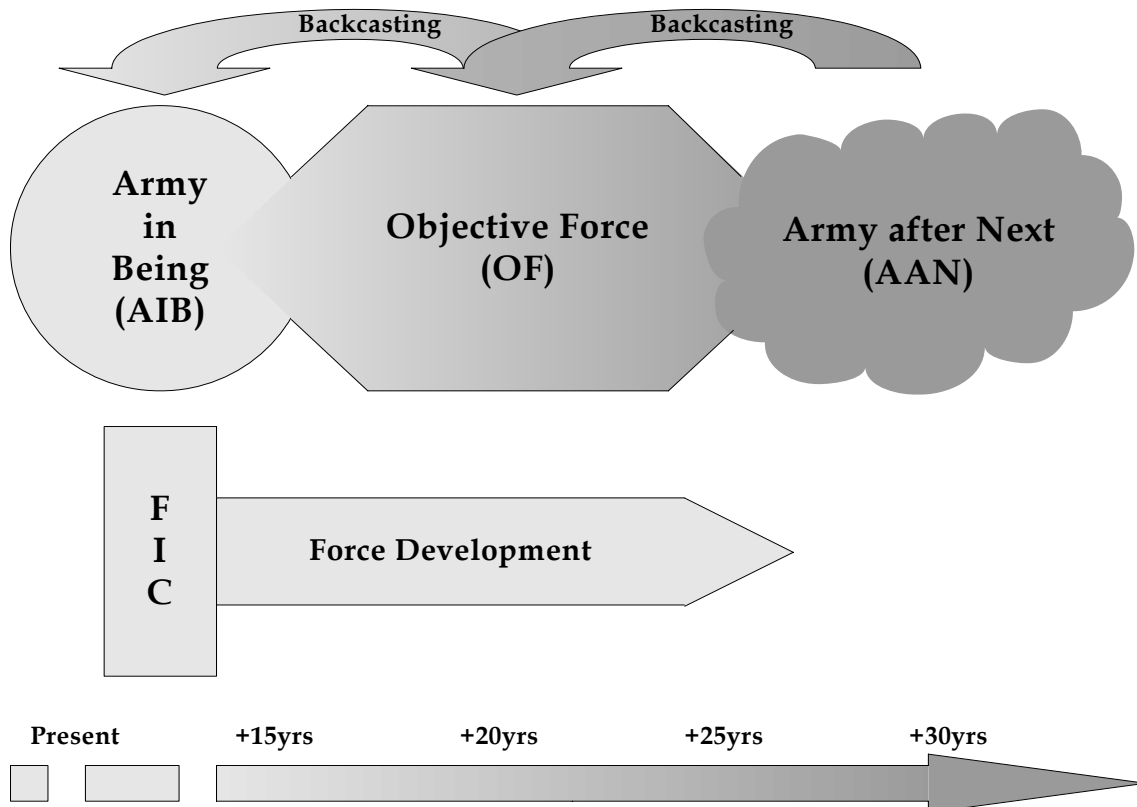


Figure 3: Army Development Continuum (from ACMP [1])

ACMP [1] takes into account the establishment of the Capability Development Group in Defence and all other activities aimed at implementing the recommendations of the Kinnaird review [11]. It emphasises the interdependence between Army and the other Services and the importance of the Army Experimental Framework (AEF). The Army Modernisation Management Section within Army Headquarters has to handle Army's involvement throughout the modernisation process. However, the direction is provided by the Army Modernisation Steering Group, previously known as the Objective Force Steering Group. According to ACMP [1], Chief of Army has delegated control of the process of modernisation and its resources to Deputy Chief of Army. Furthermore, at Army Headquarters, Future Land Warfare has to provide conceptual leadership, while Preparedness and Plans – Army manages current capabilities.

* The Hardened and Networked Army (HNA) is an interim force structure between the AIB and the OF, which has been backcast from the OF.

Army's modernisation envisages that, *at any given point in the future, we have an Army capable of successfully conducting the types of operations required of it, in the prevailing strategic and physical environment, in accordance with endorsed Government policy* [1]. However, the responsibility for contribution to Army's modernisation extends beyond the Army chain of command. Numerous elements in Defence contribute to the modernisation process at various stages. ACMP plays an important role in establishing the basis for coordinating the development effort necessary to achieve Army's desired warfighting outcomes. The objectives of ACMP, here quoted as in [1], are to:

- 'provide future warfighting concepts to guide the development of future force structures in a joint context;
- link the future warfighting concepts to the capability development effort of key land force agencies;
- employ an experimental framework tested in a joint framework to develop and refine future concepts and force options;
- detail the requirements and responsibilities for development plans and reports for outputs and new Army's capabilities;
- provide the basis for the Army to contribute positively to capability development and future capability planning in joint and wider fora in Defence;
- integrate capability implementation to ensure realisation of synergies between modernisation initiatives;
- integrate capability transition to ensure outputs required by Government are maintained at agreed levels; and
- identify Army's capability development priorities, potential vulnerabilities and potential high pay-off areas to inform and focus information collection by staff and agencies such as the Defence Science and Technology Organisation, the Defence Intelligence Organisation, etc.'

An outline of the current ACMP is given in Enclosure 1 to [1]. It follows the same Defence five-phase capability systems life cycle model, hence only the major new points will be mentioned:

- ACMP starts with the Defence Planning Guidance. It is drawn from existing strategic planning documents and processes and contains the broad tasks that Defence might face in the future;
- The Joint Warfighting Concepts come next and include Force 2020 (replaced by OF 2025), the Future Warfighting Concept called Multidimensional Manoeuvre and the Future Joint Operational Concepts that are in preparation. Below the joint concept are service-led concepts, in the case of Army the Future Land Operational Concept called Complex Warfighting;
- The AEF activities include also the consideration of capability and technology demonstrators. These are projects run by Defence and Industry to show how technology may enhance capability in a novel way;
- Currently*, the Chief of Army's Development Intent is to *develop a Hardened and Networked Army that is capable of Complex Warfighting, using combined arms effects at the small team level to generate a capability for close combat in complex terrain* [1].

* The HNA has already been endorsed by the Australian Government and there is a plan for its implementation in the period 2006 – 2015; for details refer to Chief of Army Directive 14/05 dated 16 December 2005.

- An Army Preliminary Capability Options Document (APCOD) is introduced and contains a list of generic options that meet the requirements of the capability gap analysis.
- An Army Capability Requirement (ACR) replaces the Concept for Employment Document (CED). The ACR represents Army's position on the requirement for a specific capability and enables the transition from design to entry into the Defence Capability Plan.
- The Capability Development Group is responsible for the development of the Defence Capability Strategy, which complements the Defence Planning Guidance.
- ACMP includes first-pass and second-pass approvals.
 - The first-pass approval marks the end of the process during which options are analysed and assessed to meet the capability gap identified in the Defence Capability Plan. Each option has to be accompanied by an Initial Business Case (IBC).
 - The focus of the process leading to second-pass approval is on presenting properly costed options for Ministerial and Cabinet decision making.

2.3 Coherent Force Development: A Review of ACMP

Although *Coherent Force Development* [10] is subtitled *A Review of the Army Capability Development Processes*, its focus is on the Army Continuous Modernisation Process, hence it is a review of the ACMP. It assesses the effectiveness of capability development in Army and identifies areas where improvements may be appropriate and feasible, including distribution of responsibility, authority and accountability. It also proposes marginal changes to terminology and methodology in order to reduce complexity and to ensure alignment with the capability systems life cycle model in Defence, including compatibility with processes at joint level.

The Review describes several recognised approaches, which are fundamental in capability development. These are:

- **Threat based**, where a threat is clearly identifiable and requirements and priorities are specifically measured against the capability of the threat.
- **Scenario based**, where a number of situations are described against which the optimum mix of capabilities can be assessed and tested.
- **Capability based**, which entails a functional analysis of the capabilities required to conduct expected future operations leading to a broad spectrum rather than a focused set of capabilities.
- **Resource based**, which provides the largest sustainable capability possible within an allocated budget and where unaffordable options, regardless of their potential, are not pursued.

The Review acknowledges that the ACMP follows only a modified version of the capability-based approach, see also Section 2.2. According to it, more emphasis is put on what 'concept-led' means, while 'capability-based' is not sufficiently well explained. Further on, the Review establishes that the ACMP has been implicitly influenced by threat perceptions and resource availability, which makes it less focused in comparison to being threat-based and resource-based. Hence, the approach to Army's modernisation is better described as concept-led, capability-based, threat-aware and resource-conscious.

The Review accepts that the Army Development Continuum, see Figure 3, is the three-stage construct for organising the exploration of future land forces. However, it adopts a shorter timeframe of around 15-20 years, thus starting with the AIB and finishing with the OF. Here, the AAN with its focus on the 30-year timeframe is discarded completely. This three-stage process appears to mirror the one adopted by the US Army, where Current Force, Future Force and Objective Force are the corresponding concepts. According to the Review, experience has shown that the complexity of force modernisation requires the identification of a land force as the development target at around year 10. This interim Objective Force can be used for experimentation purposes and clearly falls into the category 'Experimental Force'. The recently introduced 'Hardened and Networked Army' is an example of such a force set initially around the year 2012.

The Review acknowledges that Army is the leader in Defence in regard to capability development and experimentation. Army has accumulated significant expertise and has been continually improving its modernisation process over the last 5 to 10 years. However, there are problem areas in the ACMP, which can be summarised as command and management issues, and process issues. The former include lack of communication and coordination, differences in directives and priorities, and ill-focused efforts. The latter include deficiencies in the gap analysis, frequent changes in terminology leading to conceptual confusions, insufficient discipline in the approval process, lack of timely and accurate information flow and experimentation in need of improvement.

From the process problems identified by the staff surveyed, the Review focuses on the following ones as the most significant:

- lack of a top level roadmap;
- gaps in capability development;
- lack of a formalised gap analysis process;
- confusion over capability development documentation; and
- 'amateur' concept and requirements development staff.

Each of the above problems is discussed, and options for improving the process are presented, which are then formulated as recommendations for consideration. They include:

- introduction of a roadmap as the basis for further development of a top level guidance document;
- development by DGFLW of the suite of Future Warfighting Concepts as a matter of priority;
- DSTO assistance provided to FDG in formalising its gap analysis process;
- changes to terminology and documentation avoided for a three year period to allow existing ACMP Capability Development Documentation to bed down and mature;
- development by DGFLW of CADI on Battlespace Operating System (BOS) lines, rather than Output lines; and
- study undertaken into the training requirements for capability development staff, who need to be professionalised.

The Review identifies the main command and management problems as follows:

- insufficient staff effort devoted to conceptual development;
- discontinuity in the process flow between concept description and requirements specification, causing friction and lack of unity of direction;
- duplication of staff effort occurs in some areas, while other areas receive no effort at all; and
- the need to respond to the Kinnaird Review, which poses both challenges and opportunities.

For improving command and management, several options are designed and their advantages and disadvantages are discussed. They position the staff effort into a better-defined chain of command and thus allow accountability and responsibility to be identified more clearly. The proposed structural changes offer an improved work coordination of disparate organisations and strengthen Chief of Army's capability monitoring and reporting function.

In conclusion, the Review acknowledges that *Army has created a very solid basis for modernisation and the process is still maturing*. There are some issues that can be addressed through relatively simple adjustment. However, there are others that require more than a marginal change to the formal Army structures. The Kinnaird Review [11] provides the rationale for more significant changes with impact on the entire Department of Defence.

2.4 Defence Procurement Review (DPR 2003)

The report of the Defence Procurement Review 2003 (DPR 2003) was formally released on 18 September 2003 and has been available [11] on the DRN since 30 October 2003. A team headed by Malcolm Kinnaird was engaged to conduct a review of all aspects of the acquisition process in Defence, including the activities of the Defence Materiel Organisation (DMO). It had to provide the Government with a report on a range of problems associated with major Defence acquisition projects, namely: budget, schedule and capability matters; process, structure and accountability arrangements; personnel issues; procurement reform; and the impact of industry strategy.

DPR 2003 recognises the achievements of the ongoing reform program in Defence and specifically the recent successes of DMO in reforming acquisition. But it establishes *that there needs to be more change; that it needs to be more rapid and more fundamental in reshaping systems, structures, and organisational culture* [11]. The report acknowledges the current difficult and high-risk international environment and identifies the alternative of not satisfying the above need for fundamental changes as a factor adding more risk to the protection of the nation's interests and the safety of its defence personnel on deployment. Furthermore, achieving these objectives depends on decisions made earlier, that defined and later acquired the necessary defence capability, which enhances the complexity of the problems. A whole-of-life management approach has to be applied and changes are needed at each stage of the capability systems life cycle (compare Figure 2 with Figure 4).

Capability Systems Life Cycle

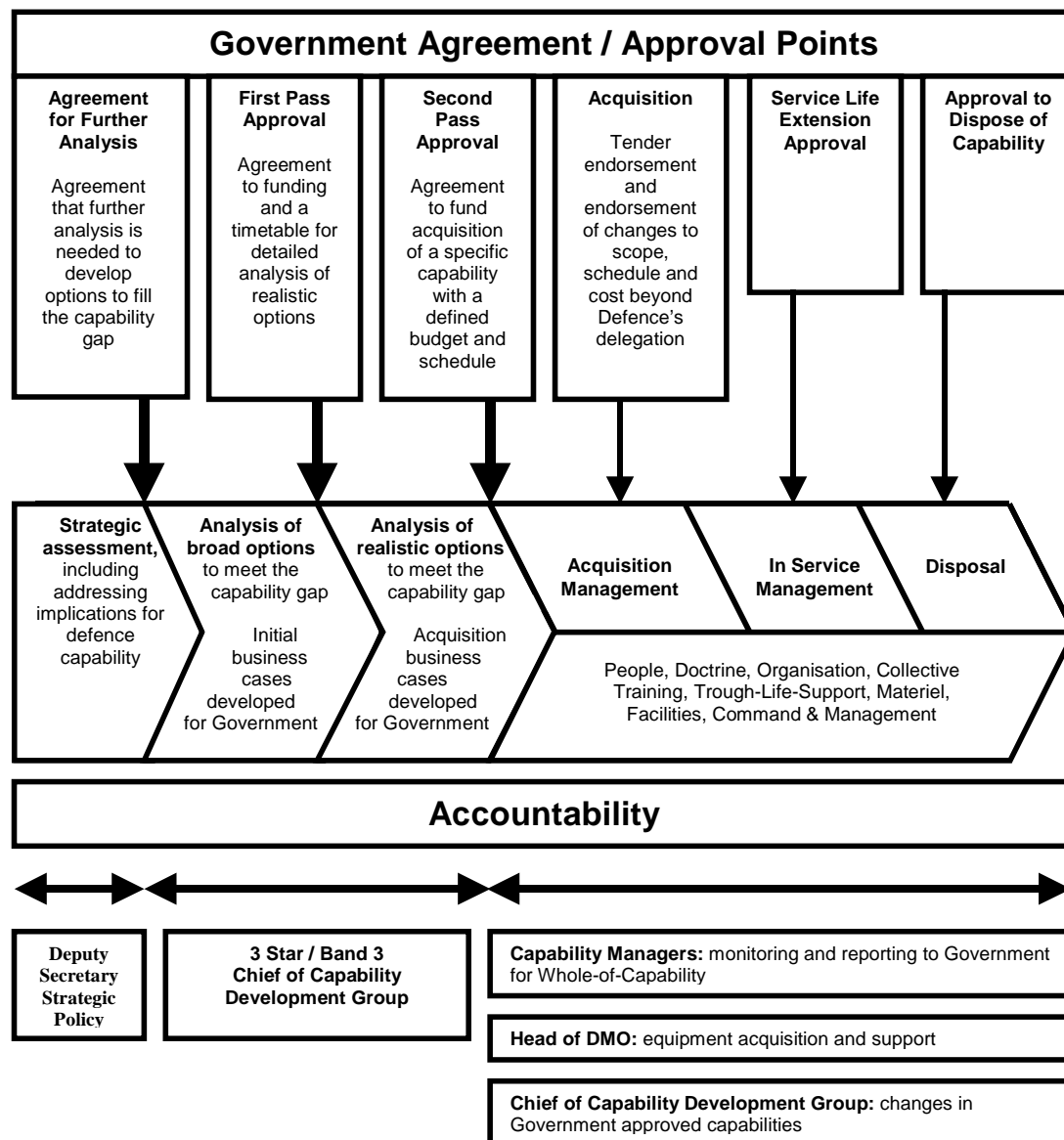


Figure 4: Capability Systems Life Cycle (Post-Kinnaird) (from DPR 2003 [11])

DPR 2003 has made, and the Government has agreed to broadly accept the following ten recommendations.

- 'Defence capabilities have to match Government's strategic guidance and hence there have [sic] to be a regular flow of information in a succinct form between them regarding assessments of potential contingencies for the ADF, the forces needed in each contingency, the capacity of ADF to provide these forces at present and in the future, and within acceptable cost levels.
- The management of defining and assessing capability has to be more focused and its accountability concentrated into a single position. This three-star officer has to

ensure a coherent, cohesive, holistic and disciplined approach to capability development.

- Comprehensive technology analyses, considerations of project cost and schedule, and earlier engagement of industry have to form the basis for a rigorous two-pass Government approval system for new acquisition.
- Government has to receive accurate and comprehensive information regarding capabilities after second pass approval and the capability managers, among them the service chiefs, are given the authority and are responsible for providing it.
- DMO has to be transformed into a more business-like organisation with the role of equipment delivery and maintenance and separate from capability development. DMO is to become a prescribed agency with greater autonomy but still within the Department of Defence.
- An Advisory Board including the Secretary, Chief of Defence Force, etc., is to be established to provide advice and support to the head of DMO and to oversee the recommendations of DPR 2003.
- Project managers within DMO have to be well qualified and highly skilled, may come from diverse backgrounds – military, industry, public service, and have to be contracted for longer time periods than current postings in Defence.
- DMO will continue accepting military personnel but [only] if they possess the necessary skills and experience that apply to all DMO staff.
- Monitoring acquisition and logistics management of approved capabilities on behalf of the service chiefs will be carried out by military staff located within DMO. However, these representatives are not to be engaged in any direct project management.
- Adopting a more business-like approach in DMO will also mean extending the role of the project governance boards to include through-life-support of defence equipment and to advise on acquisition and sustainment issues.'

DPR 2003 [11] adopts the view that, *the concept of defence capability involves more than fighting platforms such as ships, aircraft, or armoured vehicles. Rather it is the combination of people, organisation, equipment, systems and facilities to achieve a desired operational effect. It also encompasses the ability to prepare and maintain operations within a designated time for a specific period. The importance of considering the entire process of developing and maintaining capability in these terms has shaped the above recommendations regarding the reforms needed in Defence. The recommendations are not prioritised and are meant to help Defence establish a framework for introducing the necessary changes. These reforms are based on a number of key principles, which are quoted here as they appear in DPR 2003 [11]:*

- 'Government must remain in control of the process that identifies and then decides which capability gaps must be addressed.
- The concept that there must be "no secrets and no surprises", has to be central to communication between Government and the agencies responsible for capability development. Government must remain confident that it has a current and accurate understanding of the progress of capability development at every stage of the cycle.
- Adequately defining and assessing capability is critically important to the success of the procurement process.
- There must be detailed analysis of the options to achieve a required military effect before adopting a platform-based solution.

- Management and reporting structures need to be clear, well understood, and, to the greatest extent possible, ensure that they align authority, responsibility and accountability.
- A higher proportion of project funds spent on early analysis to improve project outcomes represents an investment that can return dividends in terms of greater certainty in regard to costs and a better understanding of project risks.
- Rigorous analysis of technology, cost and schedule risks, backed by external verification, is essential before any project is put to tender.
- Costs of a defence capability must be assessed on a whole-of-life basis.
- The development of a more businesslike culture will support the transformation of the DMO into a professional project management organisation.
- Skilled project managers, backed by accurate and reliable systems, are an essential prerequisite for being able to deliver projects on schedule and within budget.
- Military personnel must be able to participate appropriately in the acquisition of equipment that their Service will utilise.
- The introduction of private sector expertise to support the leadership of the procurement agency will accelerate reform.'

However, these principles may generate some difficulties in the implementation of the capability life cycle process, which includes potential restricting of initiative due to Government control of the capability development process and higher expectations associated with the level of certainty of project outcomes.

DPR 2003 recommends the adoption of the Technology Readiness Levels (TRL) approach to analysing and reporting on *technology feasibility, maturity, and overall technical risk* [11]. They have to be used to evaluate capability systems and sub-systems at various stages of their life cycles. The TRLs allow technical risks for any capability option to be identified and assessed early enough while passing through the approval stages. The proposed list includes nine levels as shown in Figure 5. The levels may be used as *benchmarks to assess the technology maturity of different capability options* [11]. The TRLs will make sure non-technical stakeholders have better understanding of the risks associated with specific capability proposals. Moreover, proposals without the technology risk evaluated will not be considered any further.

DPR 2003 suggested significant changes for the role of DSTO in defence procurement. DSTO is to be involved throughout the whole life cycle management process and especially in its early stages. DSTO's participation in capability definition and assessment is *critically important to the success of the procurement process* [11]. However, the role of DSTO will go beyond the scope of traditional activities, such as analyses and studies. In particular, the organisation is to provide effective quality assurance in relation to technology readiness. DSTO is to use the TRLs methodology to evaluate technology risks for emerging capabilities. The implementation of DPR 2003 identifies the Chief Defence Scientist as the capability development authority for technical risk; see [11] for details. DSTO has already established a 'tiger team', which has developed guidance in the area of technical risk assessment [13], [14] and [15].

DPR 2003 identifies test and evaluation (T&E) as *an essential tool in the acquisition of defence equipment to reduce risk, define technical limits and monitor contract performance and compliance* [11]. T&E can and must be applied as early as possible in the capability systems life cycle. Issues identified early allow timely rectification and lead to significant

cost savings. Also, T&E is needed to establish that the delivered equipment fulfils the Government endorsed requirements and closes the existing capability gap. Hence, T&E has to be conducted in a comprehensive and systematic way and allocated greater resources of the project funding. DPR 2003 recognises that each of the Services conducts T&E activities, but their efforts have *to be integrated with the significant expertise and experience available in DSTO* [11].

1	Basic principles of technology observed and reported.
2	Technology Concept and or Application formulated.
3	Analytical and Laboratory Studies to validate analytical predictions.
4	Component and or basic sub-system technology valid in laboratory environment.
5	Component and or basic sub-system technology valid in relevant environment.
6	System sub-system technology model or prototype demonstration in relevant environment
7	System technology prototype demonstration in an operational environment.
8	System technology qualified through test and demonstration.
9	System technology 'qualified' through successful mission operations.

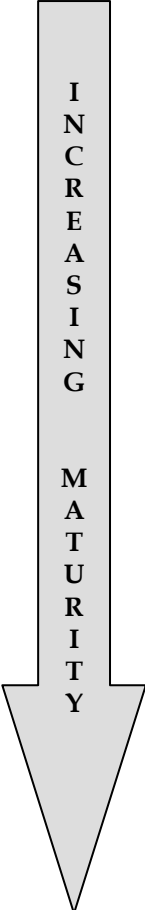


Figure 5: Technology Readiness Levels (from DPR 2003 [11])

2.5 Army Science and Technology Requirements and Priorities

Army Science and Technology Requirements and Priorities 2005-08 (ASTRAP 05) articulates Army's requirements for scientific and technological support in the context of the Army Development Continuum [12]. ASTRAP 05 informs science and technology (S&T) suppliers in Defence, industry and academia of Army's requirements and priorities given the short, medium and long terms. Thus Army uses ASTRAP 05 as a mechanism for managing its S&T support. In [12], Army recognises the importance of S&T for its warfighting capability and states its commitment to implement S&T results in the process of Army's modernisation. Scientific and technological support is required and can contribute to all phases of the Army CSLC process as shown in Figure 6.

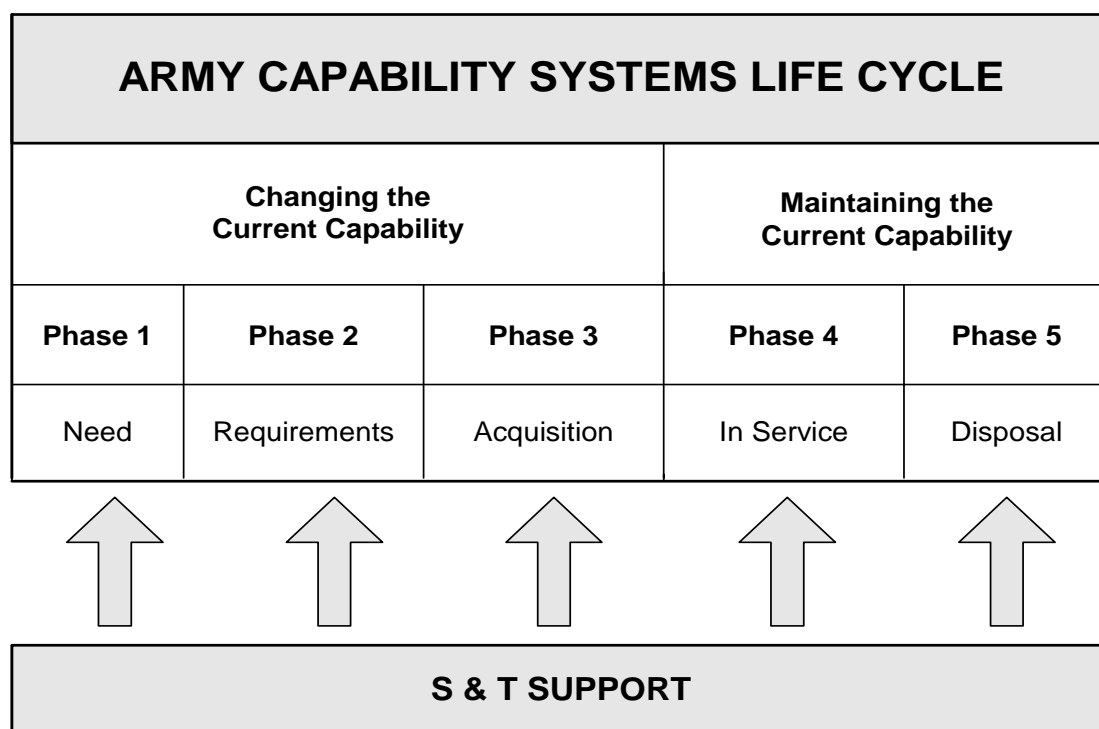


Figure 6: S&T Support for Army CSLC Process (from ASTRAP 05 [12])

ASTRAP 05 states the maximisation of the benefit to the Army from S&T investment is one of the key strategic S&T objectives. This may be achieved in particular via the employment of operational analysis [12]. Effective operations research (OR) offers the Army a mechanism to be both a smart buyer and a smart user of capabilities. In a resource-constrained environment, the selection of the most cost-effective capability for the Army is critical. OR supported by simulation and modelling, can provide improved cost-benefit analyses, better statements of requirement, and more comprehensive trade-off analyses.

Technologies emerging at present and in the future may enhance significantly Army's capabilities. The successful incorporation and exploitation of these technologies is one of the other keys to optimising the effectiveness of limited manpower and resources, and to realising Army's long-term capability goals. However, the timely and effective utilisation of advanced technology requires the effective implementation of S&T support in the form of forecasting, backcasting, modelling and experimentation. These processes are necessary to verify and validate the effectiveness of the acquired equipment and concepts of operation. Technological development is subject to on-going evolution and development, sometimes directly in defence related areas, but for the most part independent of defence applications or interests. Irrespective of the circumstances of their generation, many S&T developments, in the longer term, offer the potential for significant impact on defence applications. ASTRAP 05 provides the mechanism for identifying emerging technologies that may have military significance in the future. The technology trends are usually distilled from international collaborative activities (ABCA and TTCP), and from Australian research programs (DSTO, DMO, CSIRO and academia).

S&T support can be undertaken against all important short, medium and long-term Army requirements. However, given the constrained budget environment a balanced

approach is adopted based on thirteen Land Force Research Area Capabilities (Land FRAC). ASTRAP 05 provides a description of each FRAC and details of the individual S&T requirements that have to be satisfied within that FRAC. Concepts and technologies are discussed in view of their impact over the three timeframes of AIB, OF and AAN, and in the context of strategic guidance and Army's sub-outputs. At the beginning the OF will share many similarities with the AIB due to the significant number of extant systems remaining in service. These legacy systems will undergo improvement and capability enhancement. Utilisation of high pay-off technologies and innovations in doctrine and organisational concepts will have to be pursued vigorously. Some new systems will also be introduced characterised by the selective employment of radical new technologies. This process has to be carefully planned and managed, and the results rigorously tested before being applied.

3. Capability Options Development and Analysis System

Prior to the introduction of the latest two versions of the ACMP, Army followed the 7-stage Army Capability Management model [8], shown in Figure 7.

Army Capability Management						
Changing the Current Capability					Maintaining the Current Capability	
Stage 1	Stage 2	Stage 3	Stage 4	Stage 5	Stage 6	Stage 7
Concept Initiation and Development	Capability Options Development and Analysis	Capability Proposal	Capability Approval	Realisation	Capability Maintenance	Termination

Figure 7: Army Capability Management (from ACMP 2001-2005 [8])

At present, the process of capability management, as mentioned in Section 2.5, is based on the 5-phase Defence and Army CSLC model depicted in Figure 6. However, the difference is mainly in the structuring, and not in the sequence, nor in the nature of the individual steps of the process.

Capability Options Development and Analysis (CODAS) marks the second stage in the former Army Capability Management model. It is an iterative process that takes into account conceptual ideas, capability requirements from future warfighting concepts, doctrine, future analytical studies, guidance, Army experimentation results, and consultations with allies. At this stage future possibilities are analysed and then their potential to meet Army's requirements is discussed. Therefore, CODAS remains an essential part of ACMP. It is not restricted to a particular phase of its own, but covers parts of the Need and the entire Requirements phase.

3.1 CODAS Fundamentals

The Army must ensure that the future capabilities it develops are at the leading edge of military thought and technology. Moreover, these future land force capabilities have to be tailored for the uncertain future environments. This development process has to balance investment under budgetary and manpower constraints in current warfighting capabilities with the ones that will be effective against anticipated future threats. There is the need for a system which can provide a comprehensive picture of capability development and a systematic approach to it in the context of present and future strategic guidance. This system must help to deliver concepts of future land forces and capability options followed by their subsequent comparative analyses. The system can improve the decision making by providing more rigour, traceability and transparency in the process.

The Capability Options Development and Analysis System (CODAS) has been designed as a system able to perform a wide range of activities [2]. It may interact with and be complemented by the AEF to form an important part of the ACMP as shown in Figure 8.

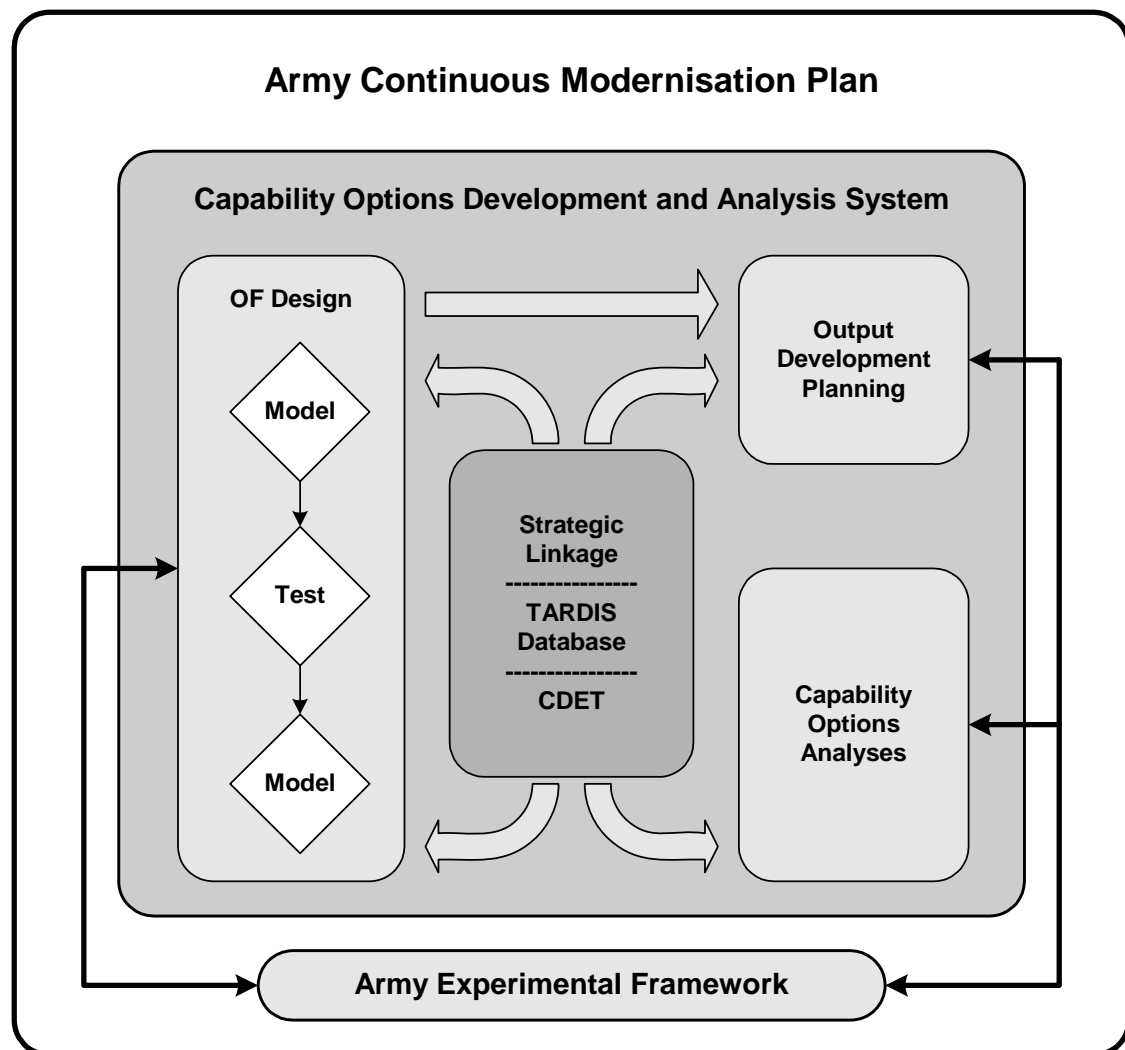


Figure 8: CODAS in relation to AEF and ACMP (from [2])

A description of CODAS includes the following attributes:

- development of a systems architecture and supporting modules that will provide the linkage between strategic requirements and potential force options;
- capability to design, test and evaluate a comprehensive description of future force options designed explicitly to meet strategic guidance;
- capacity to make comparative assessments of competing capability options;
- ability to determine the migration path and associated development plans between current capabilities and potential future options;
- analytical subsystem that supports assessment, evaluation and validation of force options and associated development plans;
- capacity to determine how various components of any future force will contribute to higher level strategic requirements through their strategic linkage;
- capacity to manage large complex datasets and report on these in an effective and efficient manner; and
- ability to highlight capability gaps and deficiencies, high pay-off areas and contentious issues so as to focus also the efforts of Army experimentation.

The central hub of Strategic Linkage, TARDIS (The ADF Requirements Development Information System) Database and CDET (Capability Development and Evaluation Toolset), represents the analytical engine room for CODAS. The OF Design, the Capability Options Analyses and the Output Development Planning are the outputs (deliverables) of CODAS, which are supported by and refined through the process of Army experimentation. The next subsections describe CODAS in more detail and summarise its architectures and processes.

3.2 CODAS Architecture

CODAS has been designed to help Army's planners solve the complex problem of linking high-level guidance with capability options. Establishing a direct link proves to be a difficult task, see [2]; hence any potential solution process has to go through an intermediate stage or stages. CODAS uses the effects that must be achieved to meet the requirements of the strategic guidance as the missing link. The employed approach appears to be systems engineering, linking user requirements with system design. The two existing versions of the architecture underpinning CODAS are presented briefly. They picture the difficulties inherent to the evolution of CODAS as a concept and as a realisation.

3.2.1 CODAS version 1

The initial version of CODAS appears to correspond to a typical strategic planning process and is based on the following three questions:

- *Why* is the process initiated?
- *What* is to be done to justify *why*?
- *How* is *what* performed?

The process is structured with the help of feedback loops between the various levels as shown in Figure 9. The requirements loop translates strategic guidance into battlespace

effects, which are to be realised and, presumably, checked against the initial high-level guidance. Next, the design loop facilitates the transition of the battlespace effects into land force options with corresponding capabilities, which in turn have to possess the potential to achieve the effects. Finally, CODAS has a confirmation loop to hold the elements of the structure together and thus link strategic guidance and force options by informing the development process and testing directly the designed land force against the strategic guidance.

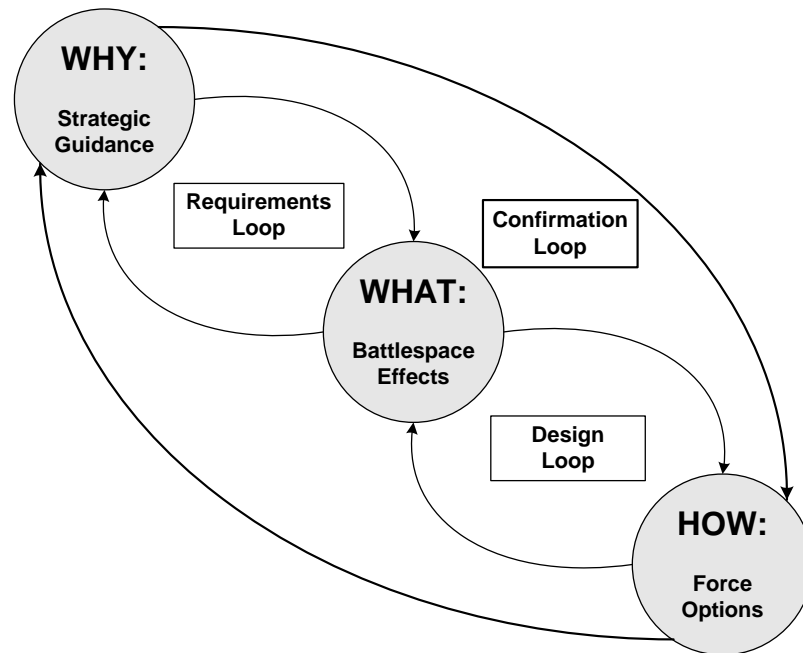


Figure 9: Description of CODAS as a System (from [2])

The structure of each constituting loop follows the same pattern and is based on the three questions: *why*, *what* and *how*, as shown by Figure 10. The process starts with the determination of the requirements necessary to achieve the battlespace effects. On the basis of the strategic guidance, scenarios are introduced to describe the future contexts and environments, in which the Army may have to operate. They clarify the need for the requirements and answer the *why* question. Then these requirements lead to *what* has to be done for the mission to succeed, i.e. to the operational objectives. The construction of the requirements loop ends with the objectives identifying sets of battlespace effects necessary for a successful outcome. The battlespace effects show *how* to realise the objectives and *how* the strategic guidance has been followed. However, there may be no unique set of effects corresponding to a particular objective. The relative stability of the set of effects may diminish further if considered against a particular scenario. New concepts and technologies may generate a different set of effects also leading to the success of the mission.

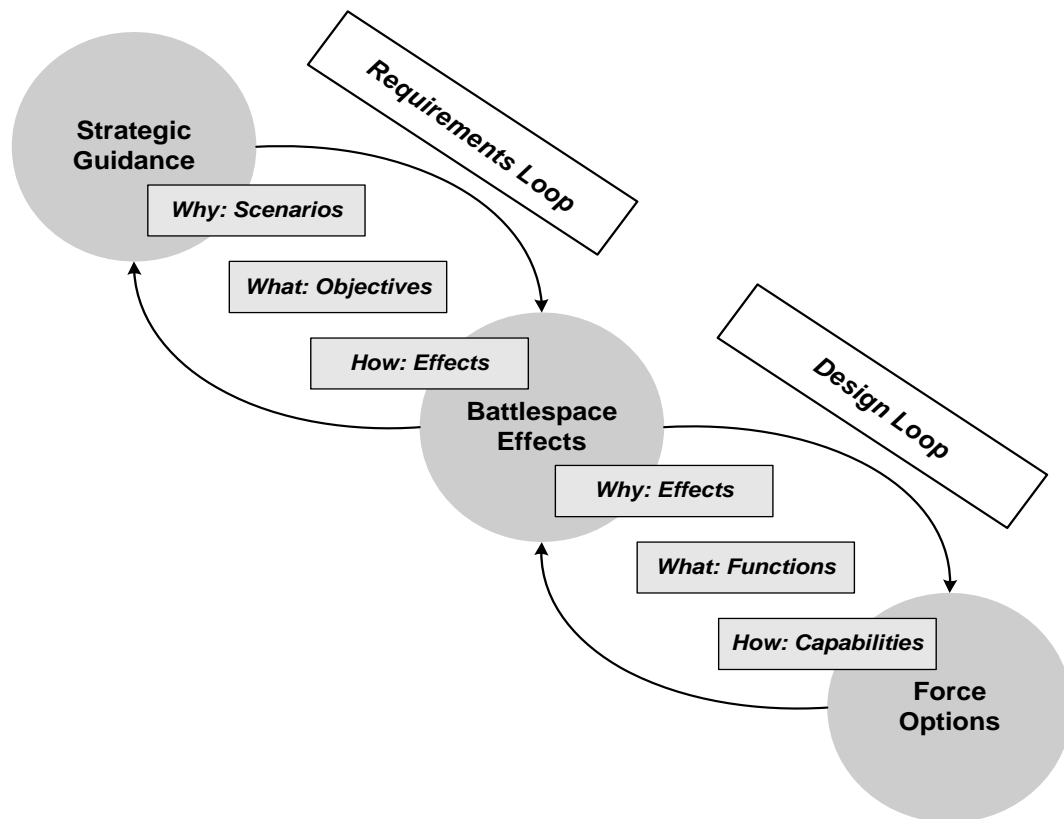


Figure 10: Systems Architecture Supporting CODAS (from [2])

The established sets of battlespace effects become the starting point and the driver of the design loop [2]. The delivery of these effects is the reason, i.e. *why* the design of force structure options with corresponding capabilities is pursued. Here, on the basis of warfighting concepts, functions are specified, which describe *what* is to be done in order to achieve particular battlespace effects. At the end, capability options are developed, able to perform the required functions. These options show *how* the effects will be delivered. But for a specific set of effects there may be a large number of options generated. Therefore, if the variety of effects resulting from the requirements loop is also taken into account, the number of chains 'guidance - effects - options' increases exponentially. However, capability-based factors may impose constraints on the force options design. Legacy systems and current capability projects may significantly influence the outcomes from the design loop. Some may be kept in service, others enhanced in capability, while the remainder are replaced with improved ones or disposed of altogether.

The confirmation loop reflects the strategic linkage, for details refer to [2], between the various components of the systems architecture and provides for the direct test of the designed land force against the high level guidance. The strategic linkage serves as the analytical environment surrounding CODAS and 'acts as the glue to hold the hierarchy' of the system together, according to [2]. It facilitates the assessment, refinement and optimisation of the force options in light of current and future operational and/or technological concepts. The strategic linkage provides for the comparison of the force options against various criteria and hence informs developers and decision makers about the relative merits of different capabilities. Establishing the ability of the force options to meet the strategic guidance by producing Output Development Plans (ODP)

and articulating migration paths for each particular FIC closes the confirmation loop. However, CODAS is an open system working in conjunction with AEF in the much wider area of the ACMP. Once CODAS has produced the final force option design, it may be subjected to extensive further evaluation, modelling and experimentation outside the system. This process may then lead to the validation of the force option and its acceptance by the Army.

3.2.2 CODAS version 2

Since the writing of [2], capability development has been the focus of several publications by Defence and Army such as [16], [17], [18], [19] and [20]. They contain further guidance for capability development, including Joint and Army operational concepts, environmental contexts and strategic guidance. This has prompted and informed modifications in CODAS to be undertaken due to the changes in the guidance. The next version of CODAS overcomes the difficulties associated with the need for defining and handling battlespace effects. It discards them as an element of the system's architecture altogether. Instead, it introduces the effects to be achieved as the joint effort of capabilities, functions and operational objectives, as in Figure 11. This approach has its origin in the definition of effects-based operations as the application of military and other capabilities to realise specific, desired operations and strategic outcomes in peace and war [21].

EFFECTS BASED PLANNING

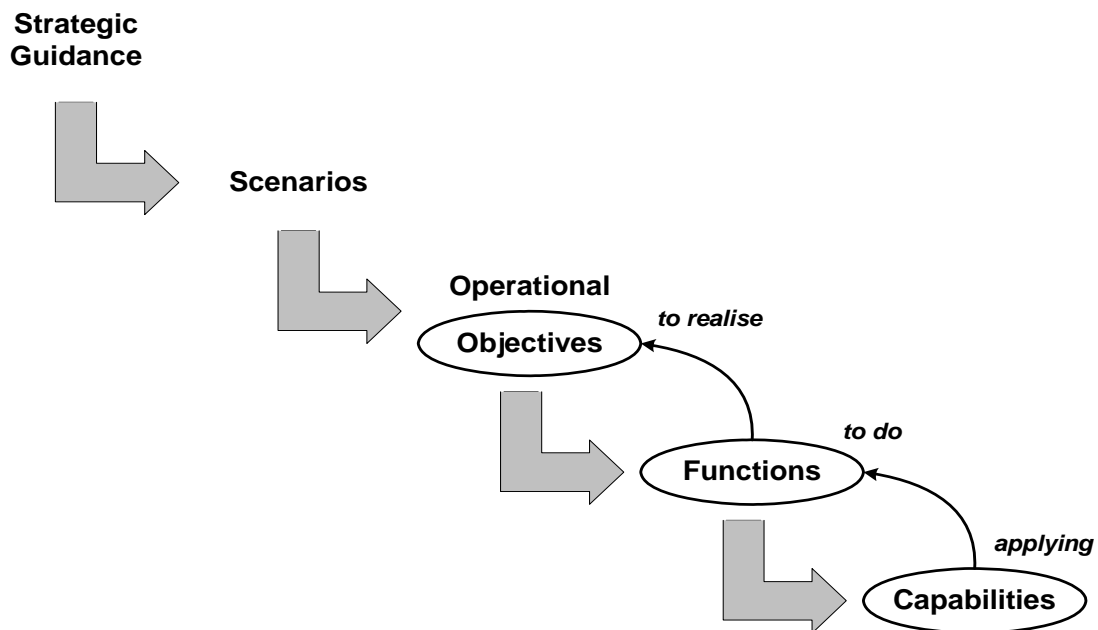


Figure 11: Achieving Effects = Applying Capabilities to perform Functions to realise Objectives (from [21])

Here, the requirements loop and the design loop are amalgamated into one cascading process. The link between strategic guidance and capability is based on the systems engineering approach [22], ensuring traceability between requirements, functional

analysis and design. However, the cascading process represents only the initial part of the systems engineering V-diagram [22]. It needs to be completed by its second verification part. Another logical alternative is to embed the cascading process within the confirmation loop replacing the requirements and design loops.

Strategic Guidance determines the various environment(s) within which the Army has to operate successfully. Moreover, recent events have confirmed the necessity for taking into account a very wide range of circumstances and contexts. Thus a large number of scenarios have to be given consideration. However, only a limited number of them can be investigated due to constraints of resources. For example, the AIPS may reduce the number of potential environments to a more manageable set. The scenarios define in turn the operational objectives to be targeted. Then, on the basis of warfighting concepts, functions are determined, describing what has to be done to realise the objectives. Further, capabilities are generated that can perform the specific functions. Here, the system focuses more on *what* needs to be accomplished rather than on *how* it is to be done, although it provides also the answer to the *how* question. The desired effects can be achieved by applying the generated capabilities to do the specified functions and to realise the given operational objectives.

EFFECTS = CAPABILITIES + FUNCTIONS + OBJECTIVES

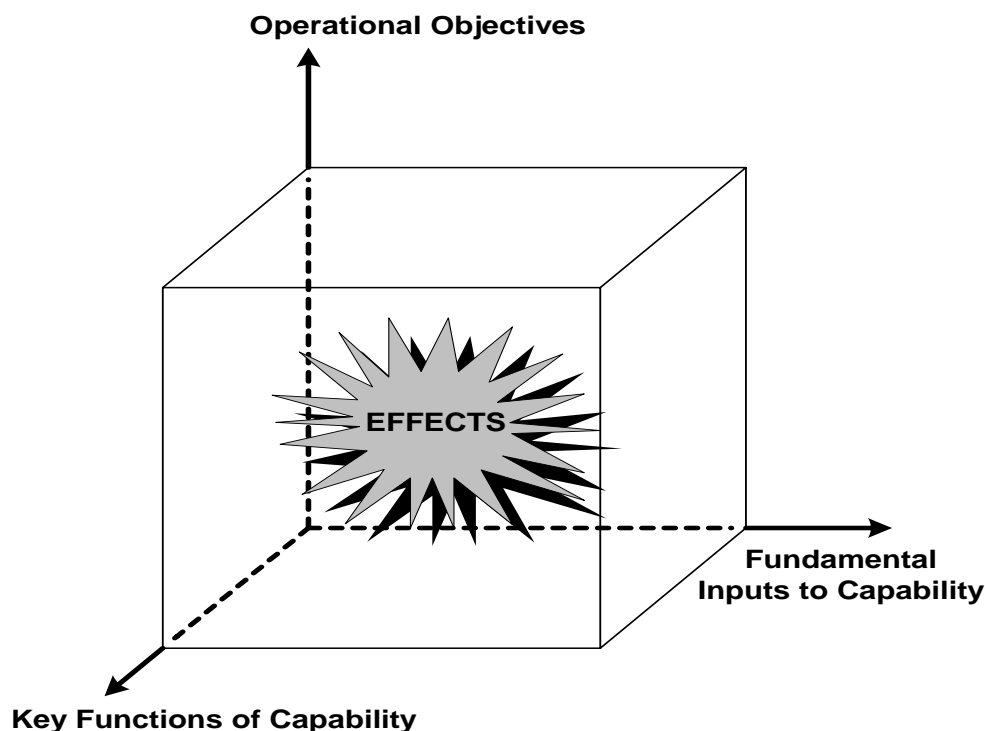


Figure 12: Effects (from [21])

As discussed in Section 2.1 any capability is delivered by a system or by systems, which comprise one or more FICs. The current Army list of FICs includes organisation, personnel, collective training, major systems, supplies, facilities, support, and command and management. Their detailed description is given in Appendix A. FICs generate

capabilities to perform specified functions as mentioned before. Army Doctrine [16] defines a function as a range of actions to be undertaken in applying force power. There are six key functions of capability (KFOC) that are essential in conducting operations. They are force generation, force deployment and redeployment, combat operations, force sustainment, force protection and force command. KFOCs represent Army's activities in creating the ability to perform designated functions on operations and achieve desired effects. Thus, the relationship between capabilities, functions, operational objectives and effects (Figure 11) can be further specified as a relationship between FICs, KFOCs, operational objectives and effects as illustrated in Figure 12.

3.3 CODAS Processes

CODAS contributes significantly to two of the major deliverables of the ACMP: the design of the OF and the production of ODPs. However, it does not target the actual end results; rather it informs and facilitates the ways and the means leading to these results. CODAS also provides for the development of capability options and their subsequent comparative analysis. It helps formulate requirements for experimentation in support of capability development. CODAS provides developers and decision makers with the ability to make better-informed and more rigorous decisions regarding future capability development. It gives them greater confidence that the decisions made will be the basis for creating better warfighting capabilities.

OF design can be viewed as a real challenge to developers [3] and [4]. It has to balance future advanced capabilities and structures characteristic for innovative warfighting concepts with extant legacy systems within the AIB, and yet it aims at producing an achievable future land force. The OF design process incorporates the following areas:

- *Effects-based design.* Necessary effects are listed as required by the strategic requirements in the future timeframe without specific reference to constraints from current realities.
- *Commander guidance.* Development intent statements by the Chief of Army and Deputy Chief of Army direct the OF parameters including limitations and constraints and require feedback at critical stages of the design process.
- *Parallel planning.* A Systems Engineering approach to the effects-based design is combined with the realities of force structure planning within the OF timeframe.
- *Stakeholder engagement.* Ongoing consultation and cooperation throughout the OF design process is maintained at BOS level and at higher Army levels.

The OF design will not necessarily include a comprehensive force description and will change over time. The OF will never be achieved and will always remain a futures concept. Thus, the designed OF is considered aspirational and potentially impossible to implement within present resource limits. The OF serves as a focus for capability development and provides a target for the concept-led production of ODPs.

Output Development Planning is a methodology for coordinating in FIC terms the introduction of new capabilities across Army's sub-outputs. It creates a long-term management framework for synchronising the capability development effort and helps prioritise decisions related to needs and resources. This is a unified and systematic approach allowing all current and future FIC management plans to be aligned and strategically guided. It provides a single authoritative data source related to capability

development, streamlines the flow of information among stakeholders and facilitates timely feedback and adjustments. For example, ACMC has to consider annual reports by FIC managers against relevant milestones.

ODPs formulate the migration paths for all FICs from the current AIB to the future OF. Hence, they anticipate the structure and capabilities of the land force at any moment of time and allow the examination of any initiatives affecting the Army within the OF timeframe and beyond. These initiatives may be divided into two broad categories: capability push initiatives and capability pull ones. The capability push initiatives reflect on all plans, projects and studies currently underway, including the Defence Capability Plan (DCP) and the Five-Year Minor Capital Equipment Program (FYMCEP). They represent the status quo and justify why Army's modernisation is capability-based. The capability pull initiatives consider future capabilities for which there exists no capability push. Since there is no current status for them, ODPs identify milestones ensuring that the required new capabilities are introduced and available at the appropriate times. The capability pull initiatives guarantee the implementation of Army's concept-led modernisation philosophy. They are investigated throughout the entire period from AIB to OF, irrespective of the existing OF design and ensure there are no avoidable gaps in Army's capabilities. ODPs give broad 'big picture' guidance and help ensure that all capability development agencies have the same view of the long-term aims of Army's modernisation.

CODAS treats the Army as a system of systems [23] and supports the development of a whole-of-force design and the necessary capability migration pathways. But this approach can be applied at levels below that of the entire Army, for example, to isolate and analyse a specific capability. Any capability is linked to the effects it creates via the functions it performs and/or the operational objectives it helps realise, and ultimately via the strategic linkage to the requirements generated in view of a particular scenario. Also a capability may be linked at FIC level to other capabilities and individual FIC elements it impacts on. Thus any capability can be treated as a system within the whole-of-force system and the Capability Options Analyses as part of CODAS applied to it.

Capability Options Analyses may examine the performance of specific capability options against the strategic requirements linked to them via a single chain of functions and objectives; or compare options with each other against a wide range of functions and objectives in the entire linkage area, as shown by Figure 13. Criteria may reflect efficiency, and effectiveness including cost-effectiveness, risk, etc. The analysis can be helpful especially when comparing current capabilities with proposed future ones. Capability Options Analyses are delivered by the applications of OR and similar quantitative and qualitative disciplines organised in the CODAS analytical toolset.

CODAS delivers also proposals for further modelling, testing and validation within the AEF and the wide area of Army's modernisation.

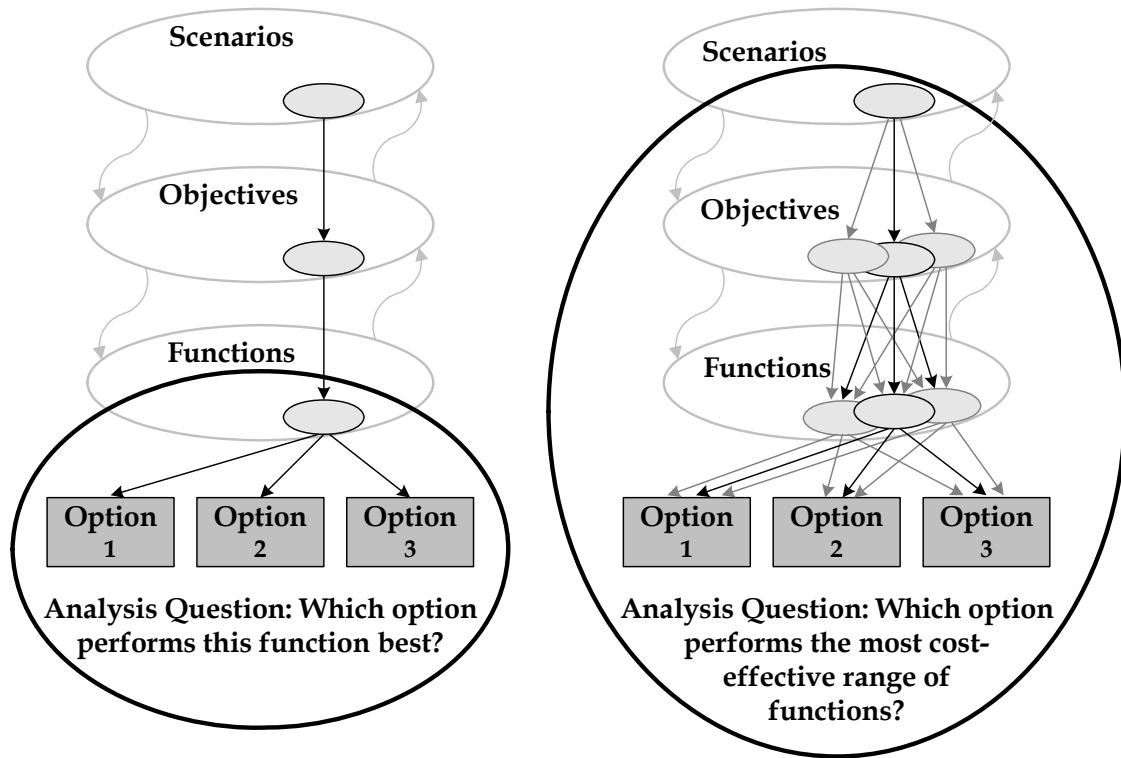


Figure 13: Capability Options Analyses (from [3])

3.4 Capability Development and Evaluation Toolset

By design, CODAS incorporates an analytical support sub-system since it needs methodologies based on quantitative and/or qualitative techniques to effectively identify, analyse and evaluate capability options of different design, 'shape and size'. For example, Subject Matter Expertise (SME) and Strategic Guidance can make essential contributions to each stage of the capability development process and have to be taken into account. The results have to be communicated in terms of already established criteria. A fully developed Capability Development Evaluation Toolset (CDET) will have the capacity to meet all these requirements and will be an inherent part of CODAS. A description, for details see [3] and [4], of what CDET will be in a position to accomplish includes the abilities to:

- capture and combine subjective ('art') and objective ('science') information;
- demonstrate options capability;
- make comparative analysis between options and/or sub-components;
- identify existing capability gaps and critical pathways, potential vulnerabilities and high pay-off areas;
- facilitate prioritisation;
- identify areas of risk and uncertainty and develop risk treatment strategies; and
- determine areas requiring further investigation.

In particular, for a specific force option CDET will be able to investigate its functional utility including:

- if it performs as expected;
- how it may be employed;
- what additional capabilities may enhance it;
- what capabilities have not been employed to the level expected;
- potential redundancies or gaps in requirement; and
- areas of risk and uncertainty in need of further investigation.

CDET is a set of a multitude of methods, tools and techniques capable of performing, for example, simulation, optimisation, resource costing, risk assessment, prioritisation, group decision support and other procedures. This is needed, because there is no single approach to solving all of the above problems. The nature of the investigation determines the appropriate choice of apparatus to provide solutions. Furthermore, CDET is expected to continue to evolve and incorporate any new method, tool or technique relevant to capability options development and analysis. CDET consists of methods, tools and techniques, which can be classified into the following four groups:

- *Development.* The elements of this group help build a model based on the needs and within a strategic context. Here capability gaps and any potential vulnerabilities are identified and handled. Quantitative methods like mathematical programming may provide a significant input, but the focus is usually on capturing qualitative data. SME plays an important role in the initial development of force options. Thematic analysis, work domain analysis, critical path analysis and the analytical hierarchy process are some of the typical development methods and techniques.
- *Analysis.* Once the initial design of a force option is completed, it is assessed whether it meets the initial requirements, performs to expectations and may compete with existing options or with other options under consideration. Further investigations may cover the impact of adding and/or removing some capability elements, potentially leading to enhanced, optimised and more cost-effective force options. Sensitivity analysis, multi-criteria decision analysis, risk analysis, cost-benefit analysis and simulation are just a few of the representatives from this group.
- *Metrics.* Capabilities have to be assessed against established performance standards and measures of merit. Unfortunately, there is no single measure applicable in any decision situation. Moreover, measures usually reflect the method used, the context of the problem, the experience of the decision maker, the availability of data and the objectives. Examples of measures include: measure of force effectiveness, measure of element effectiveness, measure of performance, and measure of outcome.
- *Data and Information.* This group relates to the inputs and outputs of the process of modelling force options. The organisation, handling and presentation of the data and information are supported by the tools and techniques from this group. Here data mining, statistical analysis, database analysis and more sophisticated object-oriented methods are needed to match the complexity of the problem.

At present [24], activities for the development of models and tools are being undertaken in a number of areas. For example:

Force Structure Design and Optimisation modelling includes: conceptualisation; data modelling; algebraic form formulation; translation by matrix generator/modelling language; presentation in algorithmic (machine-readable) form; and problem solution and solution analysis. Currently, the focus is on the following force design conceptual steps:

- determine Army's tasks and contingencies with their characteristics, likelihood and impact;
- develop alternative strategies for defeating or neutralising contingencies as each strategy involves a warfighting concept, a force design and a response time;
- determine the probability for success and the impact lowering factor of a strategy;
- satisfy Army's rotation model and combat sustainment requirements;
- determine an optimal force structure for different budget scenarios;
- prepare selected force designs for higher level consideration.

Group Decision Support System includes: building a model structure for assessing, comparing and prioritising capability options; using strategic guidance to build a hierarchy of objectives, goals and value criteria (measures of merit); using AIPS and CADI statements to put strategic guidance into context; determining the effects needed to neutralise or defeat the threats in AIPS; specifying the type and size of force capabilities required to generate the effects; and formulating alternative strategies to deal with contingencies.

DOORS (Dynamic Object Oriented Requirements System) Database Assessment and Architectures includes: assessing DOORS database management capabilities; providing architecture for integrating CDET tools into TARDIS database; and providing a framework for documenting CDET activities within TARDIS database modules.

Risk Management includes: reviewing risk management practices in Defence; establishing a framework for risk management in force capability development; developing a tool to support risk management in force capability development; and integrating the risk management tool into CODAS. Here, a *tool for risk analysis and management* does not stand for a single tool, but for guidelines, i.e. it means the methodology of applying risk management, not a specific technique, software product, etc. This methodology has to show what risk management activities and in what areas of force capability development have to be carried out and in what sequence.

Agent Based Distillations includes: identifying and developing a set of agent based distillation (ABD) models; and building a prototype ABD modelling capability and demonstrating its usefulness in concept exploration and force structure evaluation.

3.5 CODAS Implementation and Further Development

The realisation of the CODAS processes at the Land Warfare Development Centre of the Australian Army is described in publication [21]. The first result of the implementation, given the strategic guidance provided by Government in its Defence White Paper, is the definition of the OF. This land force model is concept-led (see Section 2.2) and is set 15 to 20 years into the future, around 2020 (now around 2025). Then the OF has been backcast to an interim force set around the year 2012, known at the time as the Hardened Army (now HNA) and taking into account all capability-based constraints linked to the present AIB. Here special attention has been paid to the traceability between capabilities and strategic guidance. Migration paths and corresponding development plans have also been produced. The external validation [25] has ensured that the products are consistent with the endorsed concepts in Defence and stand up to intellectual scrutiny. Ultimately, see [21], these activities have significantly influenced land force capabilities in the latest revision of the Defence Capability Plan.

ForceOp [26] has been developed to assist Army in the process of allocating force elements to different objectives of a mission. This is a mathematical programming model that uses the concept of force elements generating effects to achieve objectives. It requires users to state objectives and then specify the effects required to achieve each objective. The force elements are then rated according to their ability to create the effects required in each objective. *ForceOp* can be used to allocate force elements to the objectives in order to maximise the effectiveness of the whole deployment. The model can provide several options if required. Moreover, user-defined allocations can be evaluated and compared. *ForceOp* may be applied to complement a human decision maker by accounting for the effects of many interacting decisions simultaneously. An initial user assessment of the model has been conducted by a sample of the prospective user group. The overall outcome has appeared to view *ForceOp* as an acceptable application. However, there are issues that will have to be addressed to improve the model, for example the impact of different weapon systems, force attrition and degradation, and personnel numbers.

Publications [27] and [28] describe the results of a case study which investigates a force mix problem within the concept of Manoeuvre Operations in a Littoral Environment (MOLE) with the help of ABDs. The specific hypothesis tested is whether a small, mobile force with high situational awareness coupled with effective reach-back munitions may defeat a significantly larger force. The results from the study have led to useful insights into the force mix problem, for example quantifying the contributions of the Armed Reconnaissance Helicopters and High Mobility Artillery Rocket System as assets to the mission success; also identifying synergies among platform and weapon characteristics such as sensor range and lethality. However, this study illustrates the potential of ABDs in distilling a problem thus providing directions for further study. This research was driven by the need to introduce modelling approaches that account for emergent behaviour arising from interactions among combatants in the battlespace. Hence, it provides for support to the development and analysis of new warfighting concepts in a timely manner utilising relatively small computing resources.

Developing a force option and its subsequent analysis is the core capability of the analytical support system in CODAS. A future land force may be structured while taking into consideration strategic requirements, operational objectives, functions and effects. This may be achieved at a specified level of effectiveness and within given constraints. A significant number of deterministic techniques may be employed to assess the force option. However, uncertainty is a major factor in future capability development, leading to the consideration of a wide range of contingencies. Thus, the need arises for approaches based on chance and probability including risk management. The results of its application may be used for comparing force options or for identifying treatment strategies for a specific force option. For example, risk management may be applied to identify and categorise factors inherent to a force option that may prevent it from achieving particular strategic and/or operational objectives. The role of risk management is discussed in more detail in the next chapter.

4. Applications of Risk Management

The Manual [7] describes uncertainty as inherent to every phase of the life cycle of a capability in Defence. Uncertainty may be linked to current and prospective strategic environments, changes in technology, capability performance and reliability, financing capability projects, etc. These uncertainties may generate risks, which have to be identified, assessed and treated, so that they do not jeopardise the management of capabilities in Defence. Inadequate measures in the early phases of a capability life cycle may lead to budget blowouts, delays in availability and substandard performance. Risk management has to be applied throughout the entire capability life cycle, but its rigorous implementation in capability development may be even more appropriate. Risk management has to be engaged as early as possible, even at the strategic planning level. Indeed, in the words of the Chief of the Capability Development Group, the proposals put to the Government should not be risk averse and *the areas of risk and degrees of risk are properly identified and managed* [1].

Defence conducts its risk management activities within the Australian Defence Risk Management Framework (DRMF), described in Appendix B. DRMF is based on a unified, systematic, organisation-wide approach to risk management. It obligates everyone in Defence to employ risk management in all activities. Hence Defence can follow a common analytical process, use a common terminology free of ambiguities and share a common decision making process. Next, examples are provided illustrating the power of this unified approach in the area of capability development.

4.1 Capability Development Analyses

The 'Need' and 'Requirements' phases of the capability systems life cycle encompass the activities referred to as capability development. Following publication [29], these activities can be viewed as grouped into three capability analyses as shown in Figure 14. A brief description of these activities follows, partially based on [3]. A similar perspective has been later adopted by the *Defence Capability Development Manual* [6] as a result of the recommendations of DPR 2003 [11].

Capability gap analysis in its essence is the process of identifying current or prospective capability gaps. They may be caused by different factors including changes of the strategic environment or changes associated with major platforms or weapon systems reaching the end of their useful life. A new or revised Government policy, short-term operational imperatives or any nascent initiatives and priorities may reveal gaps in Defence capability systems. Analytical studies and joint military experiments may lead to the identification of current and prospective capability gaps, determine priorities for the order of their reduction and formulate potential ways of closing them.

The Manual [7] breaks down the capability gap analysis process into four stages.

1. The first stage is associated with the description of how future strategic and operational tasks will have to be carried out and the broad range of capabilities required.
2. The second stage deals with the level of task performance and especially the potential degradation, given current and prospective capabilities.

3. At the third stage, assessments are made of future acceptable level of task performance and of the risk of not being able to perform to that level.
4. In the fourth stage, options are discussed regarding the possibility of improving the way current and approved future capabilities might be used, or, if this is impossible, what capability options should be developed. Here, prioritisation may be conducted based on cost and risk.

CAPABILITY ANALYSES

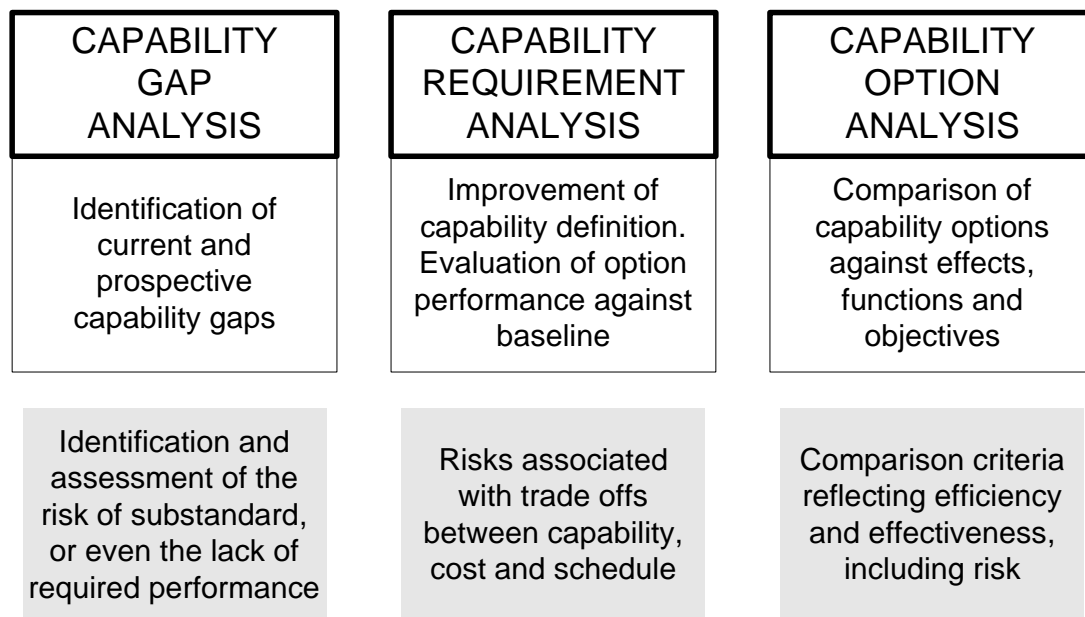


Figure 14: Capability Analyses and Risk Management (from [29])

Capability requirement analysis is the process of making further improvements in the definition of a specific capability option generated by the capability gap analysis. The focus is especially on evaluating the required performance of the capability against effects, functions and objectives, and ultimately its baseline. Analytical activities based on OR methods are used here to define and refine the requirements for reducing current or prospective capability gaps. The Manual [7] emphasises the importance of adequate effort applied at this stage including finance and resources, because of the potential prohibitive cost of correction actions later in the capability life cycle. Shortcomings, that are not identified here, represent risks, which will emerge much later during testing and evaluation for validation. The key risks, in need of attention during capability requirement analysis, are associated with the trade-offs between capability, cost and schedule.

Capability option analysis is the process of comparing options between each other against various effects, functions and objectives. Criteria may reflect efficiency, and effectiveness including cost-effectiveness, risk, etc. The analysis can be helpful especially when comparing current capabilities with proposed future ones. Capability Option Analysis is delivered by the applications of operations research and similar quantitative

and qualitative disciplines including risk analysis. Actually, capability requirements analysis and capability options analysis, as discussed above, form the two CODAS versions of Capability Options Analyses presented in Section 3.3.

As an example of these capability analyses in action, and specifically the application of risk management, we refer to the study described in [30]. It presents the preliminary analysis preceding the potential acquisition of direct fire guided weapon (DFGW) systems by Army. Firstly, the investigation addresses the choice of a broad capability option to best support future operations and the adequacy of the above DFGW systems. Secondly, a comparative analysis against stakeholder requirements determines a short list of options for further examination. The report also provides risk management related to the maturity of the technology and the quality of the information available to the study. Risk assessment for the performance of the different options and recommendations for risk treatment are also included.

4.2 Risk Management Implications from DPR 2003

DPR 2003 acknowledges that *no major project, whether it is undertaken within the private or the public sector, can be risk free* [11]. Moreover, risks have to be managed at the strategic level, even before projects are introduced. The Department of Defence has to provide the Government with response options to every reasonable contingency and the risks involved. This will inform the Government decisions regarding the military options available in such situations in terms of feasibility, time and money. Also it will allow the early consideration of potential capability gaps.

DPR 2003 establishes that lack of rigour and discipline in the process of capability definition and assessment is the principal flaw in procurement. A two-pass approval system in the early stages of the capability system life cycle complemented by *external scrutiny and verification* is recommended [11]. The first pass stage will generate options meeting the identified capability gap in the context of the Government strategic assessments. They will be presented as Initial Business Cases and provide Government with realistic capability, cost, schedule and risk trade-offs for consideration. The second pass stage will subject the options approved following the first pass to rigorous analyses and detailed studies. This will lead to the development of an Acquisition Business Case for each option. Each case will include a description in functional terms of the equipment to be acquired and will be supported by budget estimates, delivery schedules and risk analysis. At the end of this stage an agreed option may be given Government approval to proceed to tender.

DPR 2003 recognises that as a project manager, the DMO must be consistent in its approach to managing the risks, which are an inherent part of any major acquisition. This is not a trivial task given that the DMO is a public service agency conducting commercial activities and is in the process of transforming its culture to focusing on outcomes and performance. A more independent identity for the DMO within the Department of Defence is recommended, with extended powers for its head to reject proposals without full cost and adequate risk analyses. However, project managers in the DMO need the knowledge, skills and experience to tackle the technical complexity and financial risks associated with project management.

Although DPR 2003 recommends a whole-of-life capability management approach, it pays significant attention to the early phases of the capability systems life cycle related

to capability definition and assessment. The Review has established that cost over-runs, schedule delays and reduced performance of acquired capability systems often result from poor analysis and planning, well before the tender process starts. Hence, the need arises for *redirection of expenditure towards a greater emphasis on analysis and project definition* [11]. This additional initial cost has to lead to savings at the later phases of the capability systems life cycle due to better cost and schedules estimates, and a better understanding of technology risks.

4.3 Force Structure and Force Preparedness

A capability in Defence, see [7] for details, can also be considered as the unity of force structure and preparedness as shown in Figure 15. Force structure includes organisation, personnel, major systems and facilities. Preparedness is a combination of readiness and sustainability, where readiness is the ability to prepare a capability for operations within a designated time, and sustainability is the ability to maintain a capability for operations for a specific period of time. Capabilities are formed into Force Elements (FE), which in turn are aggregated into Force Element Groups (FEG). Each capability is assigned a level of operational readiness. The level of capability maintained by an FE or FEG should be consistent with its assigned readiness notice and depends on the availability of trained personnel, the availability of major platforms, combat systems and supplies, and the standard of collective training.

DEFENCE CAPABILITY

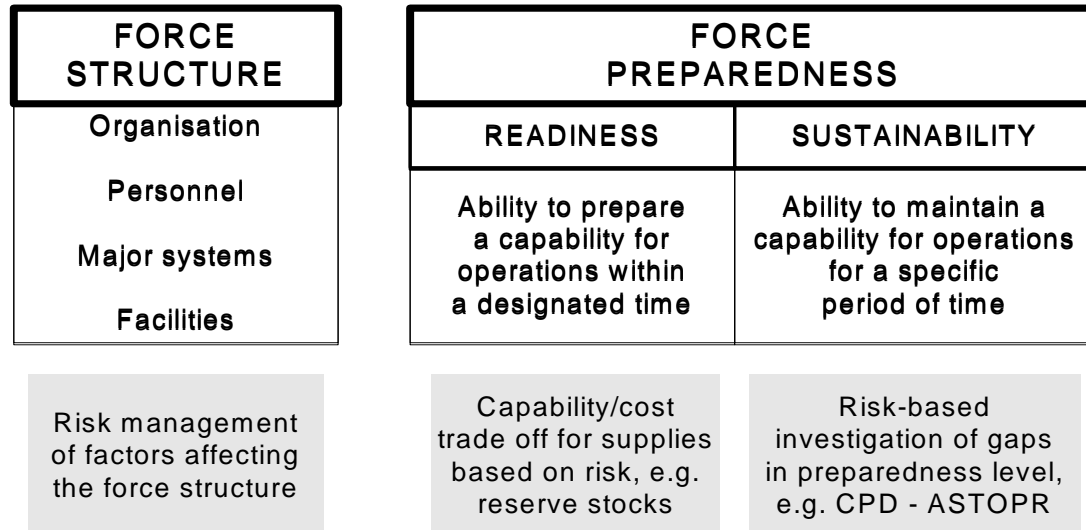


Figure 15: Applicability in Defence Capability (from [29])

Land Command 2003 is Army's plan to provide a force structure for AIB 2003*. It incorporates a force rotation model, which is expected to be a challenge for Army's existing practices for raising, training and sustaining new forces. A formal review [31] has been conducted based on FICs and risk analysis of the factors and variables expected to affect the implementation of the planned model. This study confirms the

* DCA Directive 5/2000 (AIB 2003 – DCA Planning Directive) is the reference for AIB 2003.

adequacy of the structure of the rotation model and identifies the major risks to be associated with personnel and major systems.

There is an essential link between preparedness and the maintaining of current capabilities [7]. The Chief of Defence Force Preparedness Directive (CPD) lists priorities and provides details for preparing the force-in-being to achieve the required strategic and operational effects, while the Australian Theatre Operational Preparedness Requirement (ASTOPR) provides descriptions of future operational tasks, readiness notice and sustainability requirements. There may be significant gaps between what is needed by the CPD and what is possible according to the ASTOPR. The reduction of these gaps may be undertaken within the capability development process by identifying them as deficiencies in the DCPG. Thus the gaps in preparedness may be investigated by using capability gap analysis based on risk. Resource constraints, especially finance, may prevent realisation of the ASTOPR, and an agreement is needed linking levels of performance and cost. The Directed Level of Capability (DLOC) formulates the annual level of preparedness for every FEG and articulates the accountabilities of each Output Executive. The DLOC provides a sound basis for risk management.

Operating stocks are used to sustain the peacetime activity levels of FEGs. Reserve stocks are held during peacetime to support operational contingencies at levels above the operating stock ones. Reserve stocks are kept at authorised levels and are not to be consumed in peacetime. FEGs use reserve stocks to reach their operational level of capability and sustain themselves on operations for a specified period of time. Establishing and maintaining reserve stocks need substantial financial investment, which may have major strategic implications. The Manual [7] treats reserve stocks as a significant capital cost and an important opportunity cost. Risk management is considered to be essential in this capability/cost trade-off. Moreover, reserve stockholding policies have to be developed and there is a recent study [32] in support of such an activity. It considers the reserve stocks of explosive ordnance (EO) in Army and estimates the quantity of EO required to meet given operational objectives.

4.4 Force Option Testing

Force Option Testing (FOT) can provide a mechanism for assessing the strengths and weaknesses of an option (or component thereof) within a group environment. It is usually based on SME of senior military officers, which is used to articulate objectives, criteria and metrics for evaluating force options and then to assess the structures against these objectives and criteria. FOT requires a given force option of a particular cost and design profile as a premise. It employs a systems architecture (as shown in Figure 16) similar to that of CODAS (see Figure 9 and Figure 10). Moreover, FOT precedes CODAS in time.

The testing process starts with the strategic requirements that Government needs the Australian Defence Organisation (ADO) to meet. Then a concept of operations is determined and a strategic objective is formulated. These form the *why* and are articulated as a scenario that captures the strategic environment. Requirement analyses then provide *what* is needed in order to achieve the *why*. The strategic objective has to be broken down into 'bite sized chunks' according to [33]. These are defined as theatre objectives, followed by mission objectives for each theatre objective. The objectives have to clearly state *what* effects are to be achieved (compare with Figure 11). A range of

indicative tasks are determined for each mission objective and used when assigning forces to objectives. A list is also prepared containing abilities essential to achieving the mission objective. Finally, the allocation process (see also Figure 9) provides the *how*, i.e. force elements from the available force option are assigned to each mission objective. Tracking multiple assignments throughout the process is recommended so that the degree of over-use of force elements is gauged.

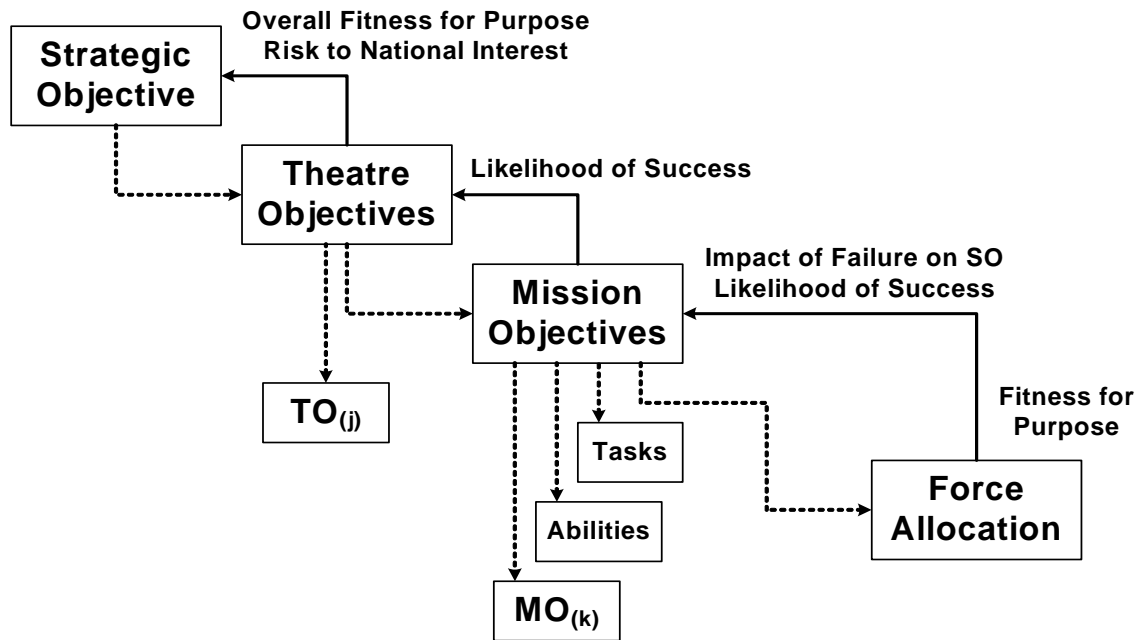


Figure 16: Summary of FOT: Method and Measures (from [34])

In order to complete the testing of the force option, the group of military experts has to make their way back up the hierarchy of objectives. At each level the experts make judgements about, and voted on the force option in terms of fitness for purpose and likelihood for success. First, the allocated force elements' fitness for purpose to achieve each mission objective is considered by discussing the functionality and capacity of the allocated force. Next, the likelihood of success of each mission objective is determined *along with an indication of the impact of failure of the mission objective on the strategic objective* [33]. Subsequently, judgements are made at theatre level for each theatre objective bearing in mind the judgements for the corresponding underlying mission objectives. Finally, at the strategic level the risk to the national interest is assessed. This risk takes into account the likelihood of failing to achieve the strategic objective and the impact of that failure. The overall fitness for purpose of the force option to achieve the strategic objective is the last judgement made. It is based on the previous judgements and some broader issues.

Publications [33] and [35] provide a guide of word pictures to inform the judgements of failure impacts. The guide has been developed to help the participants in determining the appropriate level of impact, namely trivial (inconsequential), minor, bearable, critical and catastrophic. These qualifications are close to the ones adopted officially by Defence and available in AS/NZS 4360:2004 [36]. However, there is no recommendation for a detailed gap analysis related to the identified failures. Also, no prioritisation of the considered force options is included.

4.5 Hardened and Networked Army

In 2003, as part of its modernisation process, the Australian Army developed a future force model. This force was set around the year 2012 and called the Hardened Army, which is now known as the Hardened and Networked Army. Following the direction of the Chief of Army [37], the Hardening of the Army initiative* [38] focused on creating a network capable force based on balanced and capable combined arms teams, a force optimised for close combat with greater protection, mobility and firepower, a force flexible in structure and less hollow. Thus HNA is intended to enhance Army's capability to carry out a wider range of potential military tasks and provide additional land force options to Government in the short to mid-term [39].

Figure 17 illustrates the placement of HNA within the land force evolutionary planning process. Here, AIB and AIB+ stand for the current Army in Being and its projection to year 2012. The HNA is the Hardened and Networked Army of the same year, backcast from the Objective Force set in 2020. Moreover, AIB, HNA and OF represent stages in the process of conceptual development of a future land force, while the plan for the transition from AIB to AIB+ is reflected in the strategic defence documents including the recently released public version of the DCP [40].

The Hardening of the Army concept was endorsed by the December 2003 meeting of the Chief of Army's Senior Advisory Committee (CASAC) and an Implementation Plan was developed†, following the coordinating directive of the Deputy Chief of Army [41]. It is a high priority for Army's modernisation effort [42].

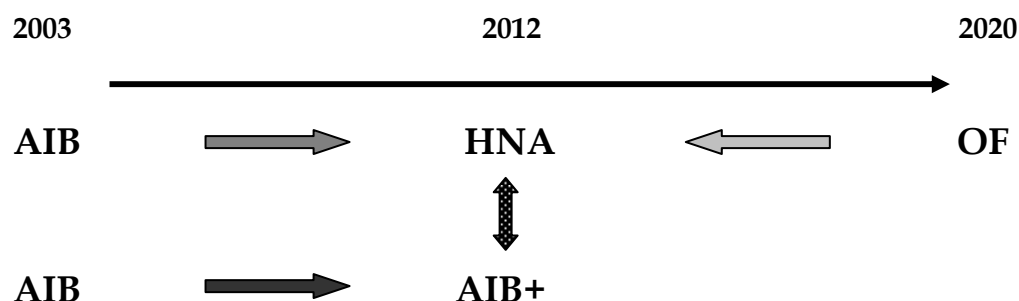


Figure 17: Land force evolutionary planning process

The actual design of the HNA was based on the military appreciation process [43]. It identified contingencies associated with the HNA, such as timely delivery of capabilities according to the DCP, and manpower and readiness levels. A study was required to inform and provide analytical support to the decision making process, which is ultimately to establish the potential of the HNA and its appropriateness. A comprehensive and systematic approach, such as risk management, was needed to assess the HNA construct and identify the potential gaps and deficiencies.

* Now this initiative is out of date.

† The HNA has been endorsed by the Australian Government and there is a plan for its implementation in the period 2006 – 2015. For details see Chief of Army Directive 14/05 dated 16 December 2005.

Here, a brief description is provided of investigation [44] requested by the Force Development Group (FDG) of the Land Warfare Development Centre (LWDC). It applied a risk management approach to identify and analyse the major differences between AIB+ and HNA. The focus was set on the assessment of the potential changes in terms of nature and degree of consequence, their likelihood of eventuating, their impact on individual HNA objectives and the assessment of the aggregate performance of the HNA.

The investigation followed the generic risk management process outlined in Figure 23. However, the emphasis was mainly on the application of the Risk Identification and Risk Analysis steps. This did not exclude the consideration of other steps altogether. For example, the initial Contexts Establishment step deals mainly with the strategic context, which includes:

- Army's operating environment with its complexity, diffusion, diversity and lethality;
- Aspects of Army's everyday business – legal, political, social, cultural, physical;
- How to align risk management with Army's mission and strategic objectives;
- External and internal stakeholders with their objectives and risk perceptions.

This step is an essential element of the 'big picture' and therefore must always be taken into account. The Risk Treatment step is also particularly important in discussing extreme risks and their treatment strategies.

The investigation was based on subjective information, i.e. judgements provided by the representatives of the BOS sections at FDG. Each BOS representative was asked to identify the differences between AIB+ and HNA considering systematically the sub-groups belonging to that BOS. The risk identification and risk analysis were based on worst-case scenarios and/or most difficult circumstances. A uniform approach was adopted based on common categories for consequence, likelihood and level of risk/opportunity. Also, consequence and likelihood had to be treated independently. Moreover, in the risk assessment phase of the process, the perception of each specific risk had to be ignored and discarded when determining likelihood. All other aspects, such as time, cost, organisation, and technology had to be considered as contributors to risk. Following a comprehensive assessment of the HNA characteristics, the FDG team agreed upon the following set of principal objectives for the comparison between the two structures:

- Increased firepower
- Increased protection
- Increased mobility
- More flexibility in structure
- Less hollowness
- Network enabled
- Meets strategic guidance
- More options to Government.

The FDG team also agreed to the procedure for generating the study input data to cover the following steps:

- Formulate objectives/questions related to a specific BOS, e.g. increased firepower
- For each HNA sub-group identify its AIB+ equivalent or best analogue
- For each HNA sub-group and each formulated objective/question:
 1. Determine *whether the consequence* of the HNA subgroup being available, compared to the corresponding AIB+ subgroup being available, *is positive or negative*;
 2. Assign a degree of consequence;
 3. Determine *the likelihood of the difference* between the HNA subgroup and the AIB+ subgroup, both capable of achieving the objective, *to occur*;
 4. Use the risk/opportunity matrix to combine likelihood and consequence into the resulting level;
 5. If the risk is in the extreme, what would be required to lower the risk and to what level?

Thus, for each specific BOS, the study input starts with the list of agreed objectives and includes a list of subgroups with corresponding risks/opportunities in terms of likelihood, consequence, level, and treatment options in case of extreme risk. Because of the unclassified nature of this paper, specific results will not be described. They are discussed in detail in [44].

A preliminary check of the consistency of the provided information was conducted, e.g. whether the correct risk/opportunity levels were assigned and whether the entries actually reflected differences between AIB+ and HNA. To keep the investigation at a manageable level, the input from the BOS sections was summarised. Entries from the same BOS and of the same risk/opportunity level were amalgamated into one if they shared some common characteristics, e.g. the same sub-group and/or they related to the same objective. Further on, a comprehensive check was carried out by the BOS representatives, so that the final set of examples for consideration provided a truly representative picture of the differences between AIB+ and HNA as agreed by FDG.

Achieving a higher level of fidelity required that the examples within each specific risk or opportunity level be prioritised. Each BOS representative conducted a separate ranking; these were then combined into a single ranking. The procedure included pairwise comparisons for all entries based on the Analytic Hierarchy Process (AHP) [45]. Figure 18 shows one of the results, where MR stands for Medium Risk.

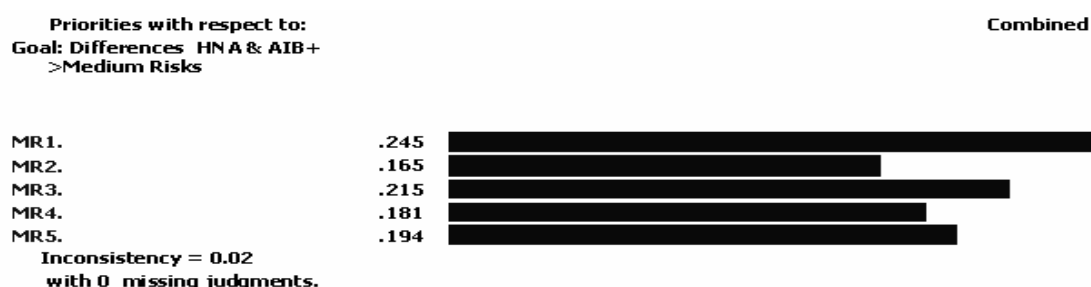


Figure 18: Example of ranked differences (medium risks) between AIB+ and HNA

Prioritising produced consistent rankings well within the AHP admissible limit. The combined results from the clustering and prioritising procedures were summarised as shown in Figure 19. The almost equal number of events with positive and negative consequences confirms how close AIB+ and HNA are as land force options altogether.

However, this study focuses more on the quality of the differences between the two structures, although their number is also important for the comparison. Figure 19 shows there are distinct differences between the two structures; the details are described in [44]. Furthermore, the large number of established differences shows that AIB+ and HNA follow distinct pathways. AIB+ is firmly based in the current AIB, while HNA is an interim OF, and a significant step towards the OF set in 2020.

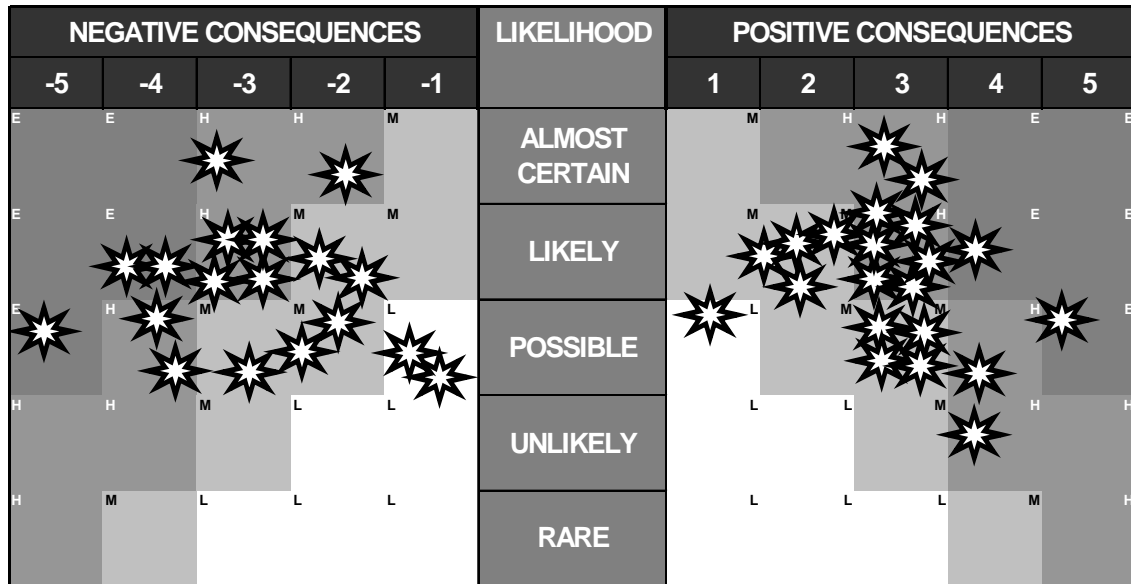


Figure 19: Summary of major differences between AIB+ and HNA

A second classification of the risks/opportunities was discussed, this time with respect to the HNA objectives, which helped to further clarify the comparison between AIB+ and HNA. Here, some events generating risk and/or opportunities were related to more than one objective. Moreover, the aggregate effect of the relevant risks and opportunities on each objective was determined. Next, conclusions were drawn on whether HNA achieved its objectives one by one. Figure 20 illustrates the relative superiority of HNA over AIB+ in the area of Network Centric Warfare.

Then these statements were combined to establish the overall positive performance of HNA with respect to the objectives altogether. Hence, HNA appears to be an improvement over AIB+, although some major risk areas need serious attention and significant treatment measures. A detailed description of these results is reported elsewhere [44].

The validity of the results from the HNA study will be significantly enhanced if it can be repeated and this time based on the SME of other important stakeholders, e.g. a group of FIC managers.

NEGATIVE CONSEQUENCES					LIKELIHOOD	POSITIVE CONSEQUENCES				
-5	-4	-3	-2	-1		1	2	3	4	5
E	E	H	H	M	ALMOST CERTAIN	M	H	H	E	E
E	E	H	M	M	LIKELY	M	M	H	E	E
E	H	M	M	L	POSSIBLE	L	M	M	H	E
H	H	M	L	L	UNLIKELY	L	L	M	H	H
H	M	L	L	L	RARE	L	L	L	M	H

Figure 20: HNA is better network enabled

5. Concluding Remarks

This document has contributed towards analysis of the CODAS, which was designed at the Land Warfare Development Centre of the Australian Army. CODAS emerged as part of the ACMP and its evolution was influenced by major events in Army and Defence such as the introduction of the concepts [17], [18], [20] and the DPR 2003 [10] and its implementation. Army used the CODAS as an analytical support framework to produce future land force options, migration paths and development plans including the OF papers and the HNA model. External validation [25] activities were conducted to ensure that the approach was sound and could stand up to intellectual scrutiny, and the results were sustainable, viable and accurate. For details in the case of HNA refer to [44]. This provides the evidence that CODAS can work and provide developers and decision makers with the capacity to make better informed decisions regarding future capability development [21].

This document has also aimed to show the potential of applying risk management to capability development in Army. The risk analysis studies of the rotation model in Land Command 2003 [31] and the HNA [44] are illustrative examples of risk management in action. Risk management has emerged as a valuable decision-making support tool in the CODAS. Although applications to date have usually been directed at reducing losses, there is the possibility of identifying and better utilising future opportunities. Risk management can be used to provide new insights and thus lead to generating entirely different options for consideration. Investigating the absolute potential of the HNA or the OF is the natural next step. The list of risk management applications described in this publication is hardly exhaustive and complete. However, it is indicative of how powerful risk management can be used as an approach to capability development. Moreover, the applications of risk management discussed in this document can be viewed as a successful application of the CODAS methodology and can serve as

confirmation of the importance of the CODAS to the process of continuous modernisation in Army.

The application of risk management in other capability systems problems can be the subject of future investigations. For example, areas of further research can include the application of risk management to the other phases of the capability systems life cycle. The acquisition phase for any major capital investment project can lead to serious risk treatment problems. Risk sharing with, and risk transfer to the private sector, and especially the public sector may generate great difficulties in the project management process. Undoubtedly, risk management applications in securing finance for major capability systems can also become a future research area. Risk management can be employed also in long-term strategic planning and development to investigate how future environments, technologies and warfighting concepts will influence capability development in Army.

6. Acknowledgements

The authors would like to express their gratitude for the helpful discussions to Lieutenant Colonel Inger Lawes, then at the Force Development Group of the Land Warfare Development Centre of the Australian Army.

Special thanks go to Dr Paul Gaertner and especially Dr Axel Bender from the Defence Science and Technology Organisation in Edinburgh who read the initial versions of this document and made numerous comments and suggestions. Their contributions have led to the significant improvement of the document.

7. References

1. Commonwealth of Australia (Australian Army), 2004, *The Army Continuous Modernisation Process* (ACMP 04/05) issued 6 September 2004. Accessed on 24 Sept. 2004 at: <http://intranet.defence.gov.au/armyweb/sites/DGFLW/>.
2. Dortmans, P. J., Jones, I. E. and Garside, D., 2003, *Scenario, Capability Requirement and Strategic Linkage: Supporting Effects-based Planning for the Land Force*, DSTO-TN-0509.
3. Jones, I. E., Garside, D., Dortmans, P. J. and Egudo, R. R. (2001) *Capability Options Development and Analysis System: An Architecture for Matching Future Land Force Capability Requirements with Current Capabilities*, Force Development Group, Land Warfare Development Centre, Australian Army (limited release).
4. Dortmans, P. J., Egudo R. R. and Forsyth, A. J. (2001) *Analytical Architecture in Support of Land Capability Development* (unpublished).

5. Dortmans, P. J., Egudo, R. R., Garside, D., and Jones, I. E. (2002) Matching Future requirements with Current Capabilities – A Systematic Approach to Capability Development Planning, Presentation to DOAS, 2002.
6. Commonwealth of Australia (Department of Defence), 2006 *Defence Capability Development Manual 2006*, Defence Publishing Service, Canberra, ACT 2600.
7. Commonwealth of Australia (VCDF Group), 2002, *Capability Systems Life Cycle Management Manual 2002*, Canberra. Accessed on 18 September 2003 at: <http://defweb.cbr.defence.gov.au/home/documents/departamental/manuals/csclm.htm>.
8. Commonwealth of Australia (Australian Army), 2001, *The Army Continuous Modernisation Plan 2001-2005*, Canberra. Accessed on 5 November 2002 at: <http://intranet.defence.gov.au/armyweb/sites/DGFLW>.
9. Commonwealth of Australia (Australian Army), 2003, *The Army Continuous Modernisation Process*, 2003 Edition. Accessed on 23 March 2004 at: <http://intranet.defence.gov.au/armyweb/sites/DGFLW>.
10. Chalmers, D. H. (2003) *Coherent Force Development: A Review of the Army Capability Development Process* (limited release).
11. Commonwealth of Australia (Department of Defence), 2003, *Defence Procurement Review 2003*, Canberra. Accessed 16 March 2004. Available at the time of writing: http://intranet.defence.gov.au/dpr-imp/15/3037_1.pdf.
12. Commonwealth of Australia (Australian Army), 2005, *ASTRAP 05 Army Science & Technology Requirements and Priorities 2005-08 (Restricted)*. Available at: http://web-vic.dsto.defence.gov.au/workareas/SA_A/index.htm.
13. DSTO – Implementation of Defence Procurement Review (DPR): Technical Risk Assessment. Accessed on August 16, 2004. Available at: <http://web-sa.dsto.defence.gov.au/DSTO/reference/DPR/tra.htm>.
14. Moon, T., Smith, J., Nicholson, J., Fewell, S. and Duus, A., 2004, *Technical Risk Assessment: principles, Process and Procedures*, DSTO-GD-0405.
15. Smith, J., Egglestone, G., Farr, P., Moon, T., Saunders, D., Shoubridge, P., Thalassoudis, K. and Wallace, T. (DSTO Tiger Team for TRA), 2004, *Technical Risk Assessment of Australian Defence Projects*, DSTO-TR-1656.
16. Commonwealth of Australia (Australian Army), 2002, *LWD 1: The Fundamentals of Land Warfare*.
17. Commonwealth of Australia (Australian Army), 2002, *Concept for Manoeuvre Operations in the Littoral Environment (MOLE) (Army's Contribution to Joint Warfighting)*.
18. Commonwealth of Australia (Department of Defence), 2002, *Force 2020*, Canberra.

19. Commonwealth of Australia (Department of Defence), 2002, *The Australian Approach to Warfare*, Canberra.
20. Commonwealth of Australia (Department of Defence), 2003, *Future Warfighting Concept*, Canberra.
21. Boey, S., Lawes, I. and Jones, I., 2003, *Army Capability Development: Linking Capability to Strategy*. In: Projected Forces, Protected Forces. Proceedings of Land Warfare Conference, 28-30 October 2003, Adelaide, pp. 77-90.
22. Blanchard, B. S. and Fabrycky, W. J., 1998, *Systems Engineering and Analysis (3rd Edition)*, Prentice Hall, Upper Saddle River, NJ 07458.
23. Curtis, N. and Dortmans, P., 2003, *The Army as a System: A Holistic Description for Technology Requirements and Analysis of Perturbations*. DSTO-TR-1537.
24. Egudo, R. (2003) *CODAS Implementation and Evaluation Support*, Presentation to DCPG Workshop, 4 March 2003.
25. Curtis, N. J., Nicholson, J. A., Nicholson, R., Richmond, M. K. and Baker, S. (in publication) *Audit of the Hardening the Army Model*.
26. Egudo, R., Boland, N. and Gan, H.-S., 2005, *A Mathematical Programming Based Decision Support Tool for Force Allocation*. In: Proceedings of the 18th National Conference of the Australian Society for Operations Research and the 11th Australian Optimisation Day, 26-28 and 30 September 2005, Perth, pp.40-49.
27. Gill, A., Egudo, R., Dortmans, P. and Grieger, D., 2002, *Using Agent Based Distillations in Support of the Army Capability Development Process – A Case Study*, DSTO-TR-1378.
28. Gill, A., Egudo, R., Dortmans, P. and Grieger, D., 2001, *Supporting the Army Capability Development Process Using Agent Based Distillations – A Case Study*, Journal of Battlefield Technology, 4 (3), pp.24-29.
29. Gaidow, S. and Boey, S., 2003, *Applicability of Risk Management in Capability Development*. In: Projected Forces, Protected Forces. Proceedings of Land Warfare Conference, 28-30 October 2003, Adelaide, pp. 439-447.
30. Davies, P. J. and Curtis, N. J., 2002, *A Preliminary Analysis of Direct Fire Guided Weapons for Project LAND 40-1 and Project 132*, DSTO-TR-1377.
31. Baker, S., Braithwaite, H., Janus, R., Nicholson, R., Philp, W., Richards, B., Shi, P., Stothard, C. and Sunde, J. (2002) *Land Command 2003 (For AIB 2003) Risk Analysis*, DSTO-CR-0238.
32. Boey, S. S., Brennan, M. J., Forsyth, A. J. and Fry, A. D. (2003) *Explosive Ordnance Reserve Stockholding – Land Component* (DSTO-TN in preparation).
33. Hodge, R. J. (2000) *Systems Thinking for Defence Strategic Planning*, Presentation to SETE 2000, 15-17 November 2000, Brisbane.

34. Hodge, R., Hendrickson, K. and Walpole, G. (2001) *Systems Thinking & Systems Engineering for Defence Strategic Planning*, 4 July 2001 INCOSE Panel Session.
35. Hodge, R. J., Wood, D. and Hendrickson, K. (2000) *A Systems Approach to Force Option Testing*, Presentation to DOAS, 16-17 March 2000, Melbourne.
36. Standards Australia/Standards New Zealand, 2004, *AS/NZS 4360:2004 Risk Management*, Standards Australia International, Sydney, NSW 2001.
37. CA Directive 05/03 – *Developing an Interim Objective Force 2012* – issued on 14 July 2003.
38. CASAC Submission on 8 December 2003 – *Hardening the Army*.
39. OCA Minute to Minister of Defence 05/03 – *Study into Reshaping Army*.
40. Defence Materiel Organisation (Industry Division), 2003, *Defence Capability Plan 2004 – 2014 Public Version*. Defence Publishing Service, DPS: NOV016/03.
41. DCA Directive 03/04 – *Hardening the Army Implementation – Coordinating Directive* – issued on 5 March 2004.
42. DCA Directive 01/04 – *Focus of Army Modernisation Staff Effort – Jan 04 to Jan 05* – issued on 3 March 2004.
43. Commonwealth of Australia, 2001, *LWP-G 0-1-4 The Military Appreciation Process*.
44. Gaidow, S., Boey, S., Egudo, R. and Lawes, I., 2004, *Assessing the Potential of the Hardened and Networked Army Using a Risk Management Approach*. In: *Weapons, Webs and Warfighters*, Proceedings of Land Warfare Conference, 27-30 September 2004, Melbourne, 393-401.
45. Saaty, T. L. and Vargas, L. G., 2001, *Models, Methods, Concepts and Applications of the Analytic Hierarchy Process*. Boston, Kluwer.
46. Department of Defence (IG Group), 2002, *Defence Risk Management Policy*, DERM, Canberra. Available at the time of this writing in electronic form at: <http://defweb.cbr.defence.gov.au/cfo/derm2/policy.pdf> and accessed also on 19 May 2004 at: <http://defweb.cbr.defence.gov.au/ig/ERM/policy.pdf>.
47. Department of Defence (IG Group), 2002, *Defence Risk Management Implementation Plan 2002-2003*, DERM, Canberra. Available at the time of this writing in electronic form at: <http://defweb.cbr.defence.gov.au/cfo/derm2/plan.pdf> and accessed also on 19 May 2004 at: <http://defweb.cbr.defence.gov.au/ig/ERM/plan.pdf>.
48. Department of Defence (IG Group), 2002, *Guidelines to Managing Risk in Defence*, DERM, Canberra. Available at the time of this writing in electronic form at: <http://defweb.cbr.defence.gov.au/cfo/derm2/guide/menu.htm> and accessed also on 19 May 2004 at: <http://defweb.cbr.defence.gov.au/ig/ERM/erminintro2.htm>.

49. Standards Australia/Standards New Zealand, 2004, *Risk Management Guidelines: Companion to AS/NZS 4360:2004*, Standards Australia International, Sydney, NSW 2001.
50. Dortmans, P., Bourn, S., Egudo, R., Gaidow, S., Hobbs, W. and D. Shine, 2004. *On the Application of Simple OR Models to the Land Force*. Presentation to 21st International Symposium on Military Operations Research, 31 August – 3 September 2004, Norton Manor, Sutton Scotney, Hampshire. Available at:
<http://www.rmcs.cranfield.ac.uk/infoserv/ISMOR/ismor2004.htm>.

Appendix A: Fundamental Inputs to Capability

The Fundamental Inputs to Capability (FICs) is the standard list for consideration of what is required to generate 'capability'. The list is to be used by ADO agencies at all levels and is designed to ensure that all agencies manage and report capability using a common set of management areas. This in turn will assist the appropriate allocation of financial resources across Defence, improve accountability and enhance the formulation of a response to a contingency, when it arises. The following information provides an indication of the scope of each element of the FIC. The detail of each element is by no means prescriptive and permits reporting flexibility from Groups.

Organisation. Every ADO agency needs to ensure it has the required personnel establishment, appropriate balance of competency/skill-sets, and correct structure to accomplish its tasks and to ensure adequate command and control. This is essentially a minimal cost activity that provides the underpinning structure for Defence. At the Service level, consideration must be given to developing flexible functional groupings that can meet contingency personnel rotation requirements and continual force improvement requirements.

Personnel. Assuming the required establishment is authorised, the positions must be filled with individuals who satisfy the necessary individual readiness requirements. These requirements include medical/dental standards, physical fitness and appropriate individual training. Each individual must have the competencies to perform the functions of their positions (both specialist and common military skills) and the motivation to apply those competencies to achieve the required performance standards of the organisation. The personnel element includes the retention and development of people to meet Defence's needs. This category includes salaries and wages, superannuation and allowances.

Collective Training applies across Combined, Joint, Single Service and unit levels. To enhance performance, organisational elements must undertake a comprehensive and on-going collective training regime validated against the preparedness requirements derived from Government guidance.

Major Systems are those that have a unit cost of A\$1m or more, and/or have significant Defence policy or Joint Service implications. They include ships, tanks, missile systems, armoured personnel carriers, major electronic systems, and aircraft. While there is an apparent linkage with Class 7 Supplies, major systems are core components of capability that regularly require more detailed reporting and management, and will be considered separately.

Supplies ADFP 20 specifies 11 classes of supply (these classes are also employed by NATO). For many items, there is a need to identify more than just quantities (eg serviceability, configuration status, operational viability resources, and reserve stockholdings). The 11 classes are:

Class 1. Subsistence, including foodstuffs, gratuitous health, welfare items, and water when this is provided in a packaged form through the supply system.

- Class 2. General Stores, including clothing, individual equipment, tentage, tool sets and kits, hand tools, stationary and other general administrative and household items.
- Class 3. Petrol, Oils and Lubricants (POL) including other hazardous liquids, chemicals and gases such as LPG and hexamine.
- Class 4. Construction Items and Materials, including all fortification and barrier materials, but excluding explosive devices.
- Class 5. Ammunition, including PGMs, pyrotechnics, propellants and fuses.
- Class 6. Personal Demand Items, including canteen supplies and non-scaled military items.
- Class 7. Principal Items. This excludes major systems as described at paragraph 4. This class constitutes a combination of end products ready for their intended use, such as most vehicles, small arms, communications equipment and training equipment.
- Class 8. Medical and Dental Stores.
- Class 9. Repair Parts and Components.
- Class 10. Miscellaneous, also known as materiel support to non-military programs.
- Class 11. Controlled Stores (Quadripartite forum only).

Facilities include buildings, structures, property, plant and equipment, and areas for training and other purposes (eg exercise areas and firing ranges), utilities and civil engineering works necessary to support capabilities, both at the home station and at a deployed location. This may involve direct ownership or leasing arrangements.

Support A widely embracing category that encompasses the wider National Support Base and includes training/proficiency support, materiel/maintenance services, communications/IT support, intelligence, recruiting/retention, research and development activities, administrative support and transportation support. Agencies that could provide this support include:

- Other Sub-Outputs;
- Output Enablers;
- Owner Support agencies;
- Civil/Private Industry/Contractors;
- Other Government agencies (eg DHA);
- International Support Base agencies.

Command and Management underpin operating and management environments in Defence through enhanced command and decision-making processes/procedures and management reporting avenues. Command and management processes at all levels are required to plan, apply, measure, monitor, and evaluate the functions an agency performs, with due cognisance of risk and subsequent risk management. Command and Management include written guidance such as regulations, instructions, publications, directions, requirements, doctrine, tactical level procedures, and preparedness documents. Consideration must be given to the adequacy of extant written guidance. Command and Management also include funding not readily attributable to any other FIC element (eg. discretionary funding).

Appendix B: Risk Management in Defence

Traditionally risk management has been applied to most activities in the ADO. The three services and some major institutions within ADO have a sound record of adopting risk management as an inherent part of their everyday ways of doing things. They have always had risk management frameworks to suit their own needs and they have their own manuals, policies, rules, plans and guidelines. Now, more than ever, in view of many events of global and local importance, the necessity for a coordinated and systematic approach to managing risks in Defence has emerged. The ADO has had to set a new higher standard of risk management, align it with Defence's strategic objectives and make it part of the business planning and decision making. Thus, at the beginning of 2002, the Secretary of Defence and the Chief of Defence Force endorsed a top-down, organisation-wide, comprehensive and systematic approach to risk management in Defence. As a result, the Australian Defence Risk Management Framework (DRMF) was established.

B.1. Australian Defence Risk Management Framework

DRMF consists of a policy [46], an implementation plan [47], guidelines [48], using existing 'best practices', and a support mechanism with corresponding funding, training and information systems.

There is an established specialised unit – the Defence Enterprise Risk Management section which acts as the focal point for any risk management activity throughout ADO. At present DRMF is being incorporated and integrated within the existing departmental management framework as shown in Figure 21.

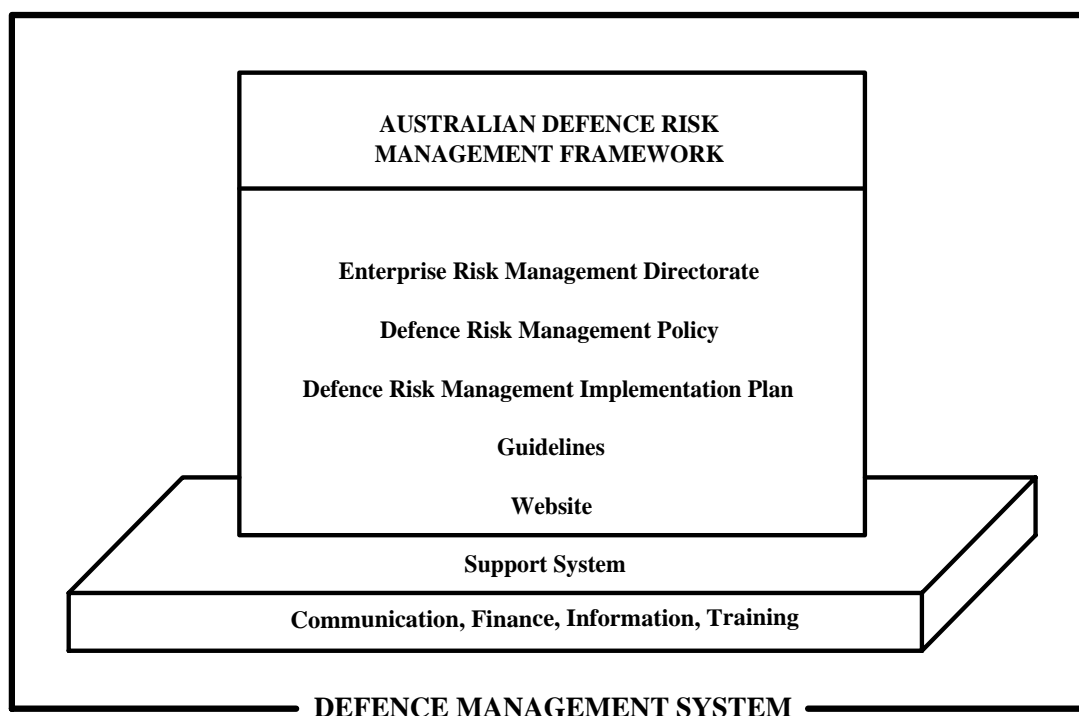


Figure 21: Australian Defence Risk Management Framework

DRMF provides for and obligates all Defence personnel to implement risk management in any activity, thus creating the conditions for an entirely new risk management culture within the ADO. Furthermore, this recent approach is directed to making better use of opportunities rather than to minimising losses or avoiding risk altogether, which has been the objective of the traditional approach.

Thus a new, more enterprising aspect of the approach is revealed. DRMF has created a solid unified basis for decision making at all levels from the individual to the key strategic, and above all to the enterprise ones, see Figure 22. Its elements are suitable for implementation by anyone in the ADO, in any sort of activity, be it analysis, training or acquisition. Risk management provides support in the decision-making process by exploring issues in an organised and structured way. It may bring clarity in current positions, uncover new insights and identify potential opportunities.

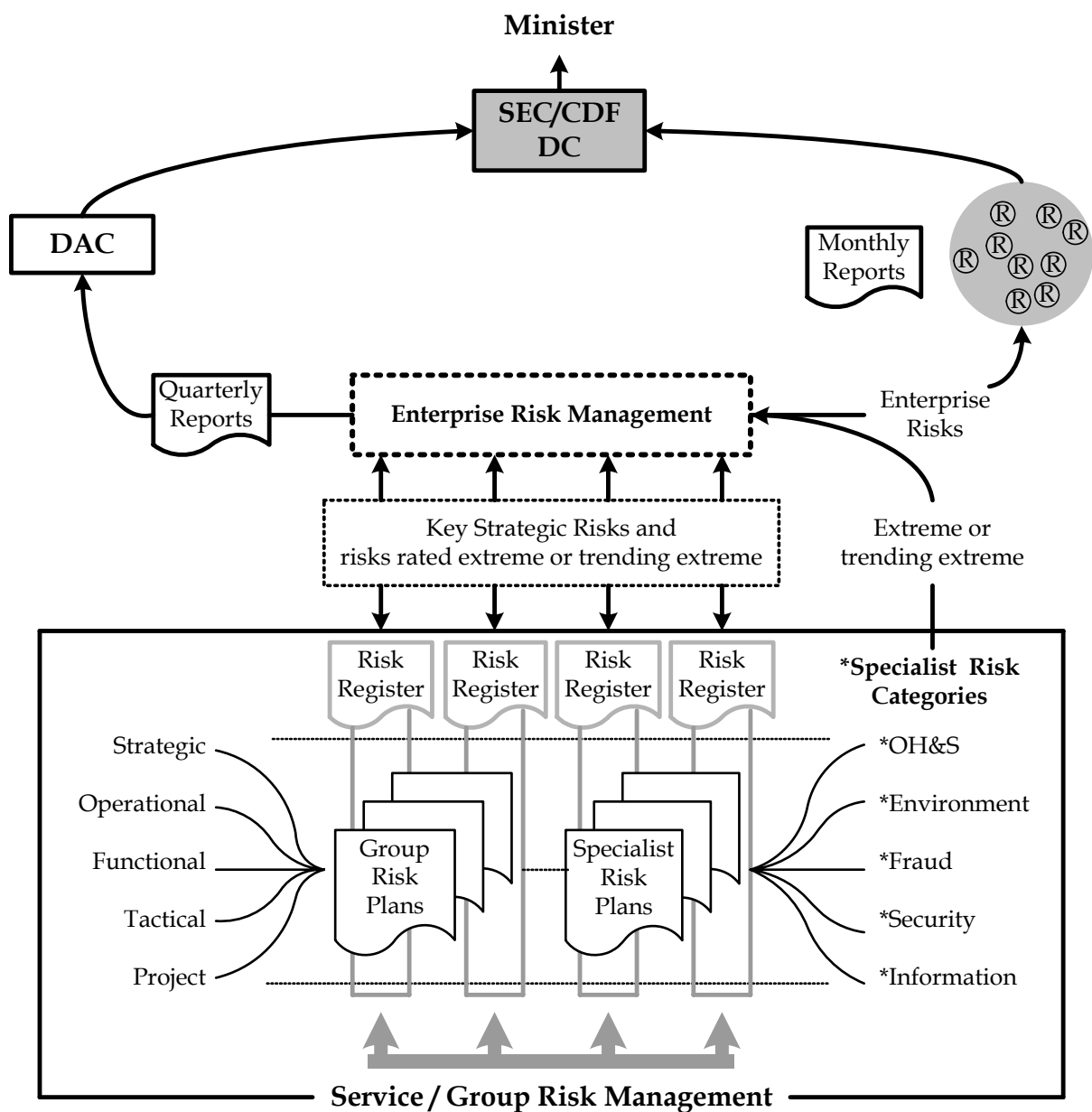


Figure 22: Managing Risks in Defence (adapted from DRM Implementation Plan [47])

The Guidelines of DRMF indicate the available analytical tools, for example SWOT, Mind Maps, Fault Tree Analysis, and Critical Path Analysis. However, DRMF does not restrict the type of techniques to be used in the risk management process. Nor does it prescribe what tool should be applied to what situation. However, different methods have to complement each other and help reveal different aspects of the same problem.

B.2. Summary of the Risk Management Process

The Australian Defence Risk Management Framework was introduced and based on *AS/NZS 4360:1999 Risk Management*. However, this report refers to the latest edition, *AS/NZS 4360:2004* [36]. The standard provides generic guidance through all steps of the risk management process: communicate and consult, establish the context, identify risks, analyse risks, evaluate risks, treat risks, monitor and review. Figure 23 shows its detailed flow-chart.

Communicate and Consult

Communicate and consult is an integral part of the risk management process. It is ongoing and lasts as long as the whole risk management process. Communication and consultation is an important process and involves a two-way information flow between all stakeholders. It is recommended to have a communication plan linking external and internal stakeholders from the very beginning and related to each step of the risk management process. Consultation has to be given priority rather than simply passing information from decision makers to the other participants in the process. Effective communication is vital in ensuring risk managers and remaining stakeholders understand the basis for certain decisions made and actions undertaken. Risk perception among stakeholders differs due to differences in interests, needs, assumptions, concepts and backgrounds. Decisions regarding risk acceptability are usually made on the basis of risk perception. Stakeholders have a significant role in the decision-making process. Therefore, it is important to have all these perceptions, and everything following from them, identified and documented. The reasons for the differences have to be investigated and understood.

Establish the Context

The risk management process takes place in the framework of the organisation's external, internal and risk management contexts.

- Establishing the external context means identifying the environment in which the organisation operates, its strengths, weaknesses, opportunities and threats. The financial, political, social, cultural, legal, public relations and physical aspects of the everyday business are very important to the organisation and its clients. This also includes the external stakeholders with their objectives and values and the key business drivers. The communication policies to be established with these parties will have to be based on that information. This helps when developing the risk management criteria later.
- Establishing the internal context is based on the understanding of the organisation, i.e. its internal stakeholders, culture, structure, values, policies, and its goals and the strategies to achieve them. It also means ensuring managers understand their role in the decision-making process with respect to risk acceptance criteria and feasibility of risk treatment options.

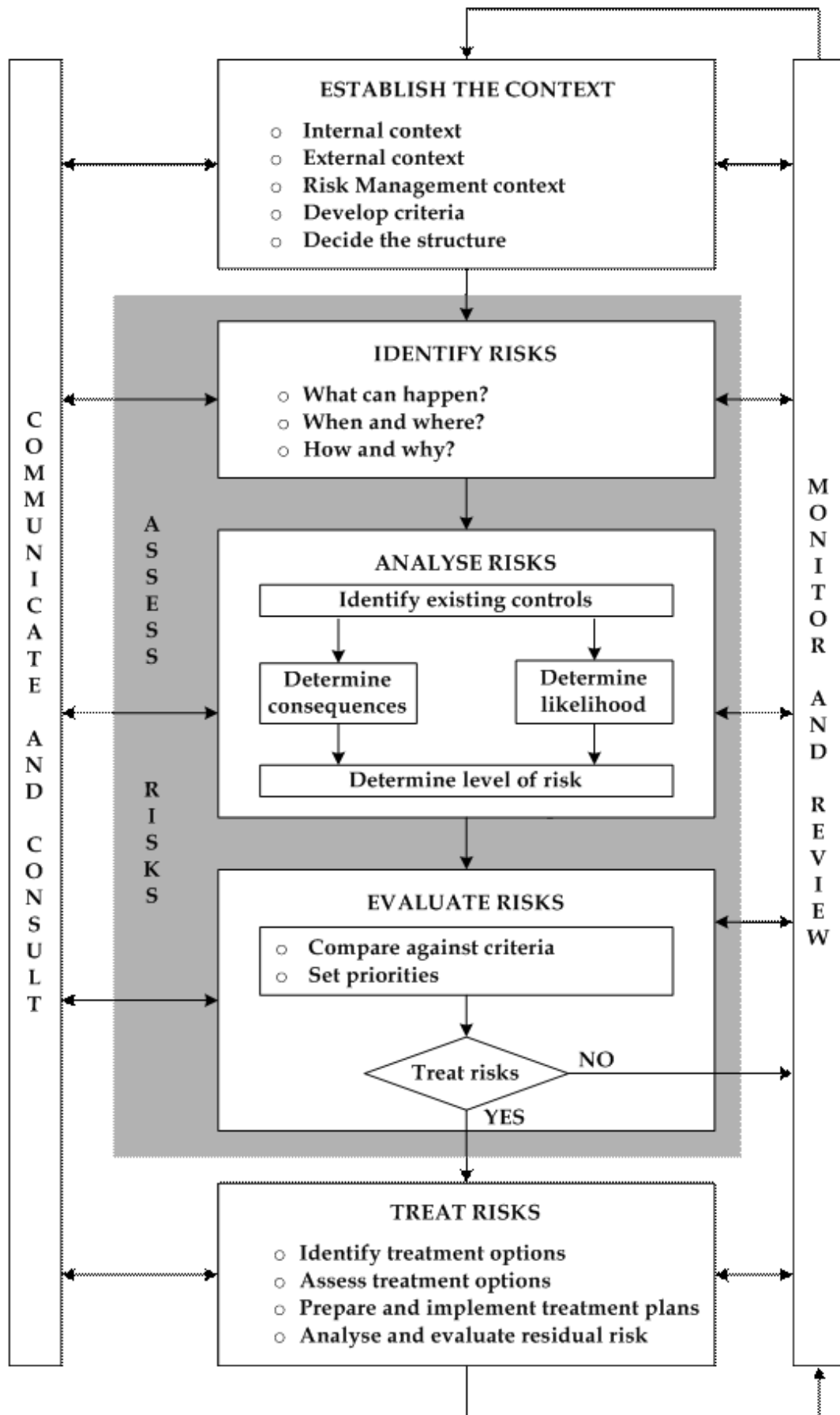


Figure 23: Risk Management Process (from AS/NZS 4360:2004 [36])

- Establishing the risk management context means considering the scope and depth of the risk investigation. This determines whether the risk management process will be concerned with organisation-wide issues or will be limited to a particular unit(s) or project(s) and their interactions. The necessary steps (including studies, tools, resources) in the risk management process are to be identified within a balanced system of costs, benefits and opportunities.

This phase involves the development of criteria against which risk is to be evaluated. The criteria usually depend on the interests of the stakeholders and the objectives of the organisation, and may also reflect legal requirements. In general, they have to reflect the contexts considered above. The nature of the criteria may be operational, technical, financial, social, environmental, legal, humanitarian, etc. Here the acceptable level for each risk has to be considered.

Risk Identification

At this step of the risk management process one has to apply a well-structured and systematic approach and try to identify all risks, which may potentially arise. Failure to do so may have a major negative impact on one's activities. Moreover, any risk left unidentified is naturally not even included in the risk management plan. Risks beyond one's control are also to be identified.

Risk identification is supposed to give answers to the following questions:

- What can happen?
- Where and when can it happen?
- How and why can it happen?

The 'What can happen?' question aims at generating a comprehensive list of sources of risk and events that may impact on the achievement of the objectives considered in the context. The impact can be positive or negative, i.e. it can facilitate, stimulate or enhance the achievement of the objectives or it can hinder, prevent, degrade or delay it. Thus, this question can be further broken down to 'What can be improved?' and 'What can go wrong?'. Hence, risks with positive and negative impacts can be later analysed simultaneously using the same yardsticks for likelihood and consequences and the same matrix (see Figure 24). This leads to a more balanced approach, especially when relative advantage/disadvantage has to be established. The 'What and where?' and 'How and why?' questions aim at considering possible causes and scenarios. Since there are many ways in which something can happen, it is important not to overlook any significant causes.

Section 5.4 from HB 436:2004 [49] provides guidance on the sources of information for identifying risks. Historical information about the organisation itself or similar organisations is considered a good starting point. Then, discussions with various stakeholders are recommended. Approaches suitable for risk identification are summarised in Section 5.5 of [49].

Risk Analysis

In this step one considers the risk consequences (impact or magnitude of effect) and likelihood (measured by frequency or probability) of risk occurrence to combine them into the level of risk. The risk level is discussed within the context of existing or non-

existing controls. Here the very low acceptable risks are separated from the major risks and excluded from further assessment.

There are three types of methods applicable in risk analysis. In order of complexity they are: qualitative, semi-quantitative, and quantitative. Usually one starts with the qualitative analysis to get a rough approximation of the level of risk and then proceeds with a more accurate quantitative analysis.

- Qualitative analysis determines consequences and likelihood in narrative form based on descriptive scales. It is applied to determine level of risk where time and money do not justify a more detailed analysis. Its appropriateness is quite evident in risk situations with stakeholders of various backgrounds, interests and mathematical/ statistical competency. Qualitative analysis is a more efficient tool when numerical data are inadequate for quantitative analysis. Sections 6.2 and 6.5 of HB 436:2004 give examples of descriptive scales for likelihood and consequences, and the resulting risk level matrix. They are reproduced as Table 1, Table 2 and Table 3.
- Semi-quantitative analysis replaces the qualitative descriptive scales with number ranges. Here numbers do not correspond accurately to the level of likelihood and consequences. What counts is the consistency in the prioritisation approach. This type of analysis is intended to be one degree more detailed, but without achieving entirely realistic assessment of risk levels. Numbers are used for comparison only and any calculations are meaningless.
- Quantitative analysis is applied when the likelihood and the consequences can be quantified. The quality of the numerical data and the sophistication of the methods used determine the accuracy of the analysis. Consequences are worded in terms of monetary, technical, or human criteria, while likelihood is presented as frequency or probability. Further, they are combined to form the level of risk and the result depends essentially on type of risk and the context.

In risk analysis some estimates lack precision, hence a sensitivity analysis of the results is recommended to test its effect on assumptions made and quality of available data. Later sensitivity analysis is applicable to test the appropriateness and effectiveness of potential risk treatment options.

Note the following:

- Section 6.2 of HB 436:2004 provides examples of quantitative and qualitative consequence scales used in relation to profits, health and safety, natural environment, social/ cultural heritage, public opinion, etc.
- In semi-quantitative and quantitative analysis, likelihood is sometimes described as the combination of frequency to exposure and probability. Frequency of exposure measures the strength of association with the source of risk while the probability measures the chance of experiencing the consequences given the source of risk exists. One has to be careful if there is a strong relationship between frequency of exposure and probability.
- This phase is based on qualitative assessment and uses narrative descriptions. The main objective is to find the right place for each event, i.e. difference in the risk/opportunity matrix shown in Figure 24.

Table 1: Qualitative Measures of Consequence/Impact (from HB 436:2004 [49])

Level	Descriptor	Detailed Description
1	Insignificant	Negligible impact upon objectives
2	Minor	Minor effects that are easily remedied
3	Moderate	Some objectives affected
4	Major	Some important objectives cannot be achieved
5	Catastrophic	Most objectives cannot be achieved

or in the case of recognising and exploiting opportunities:

Level	Descriptor	Detailed Description
1	Insignificant	Small benefit, low financial gain
2	Minor	Minor improvement to image, some financial gain
3	Moderate	Some enhancement to reputation, high financial gain
4	Major	Enhanced reputation, major financial gain
5	Outstanding	Significantly enhanced reputation, huge financial gain

Table 2: Qualitative Measures of Likelihood (from HB 436:2004 [49])

Level	Descriptor	Detailed Description
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur at some time
E	Rare	May occur only in exceptional circumstances

Table 3: Qualitative Risk Analysis Matrix (from HB 436:2004 [49])

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Medium	High	High	Extreme	Extreme
Possible	Low	Medium	High	Extreme	Extreme
Unlikely	Low	Low	Medium	High	Extreme
Rare	Low	Low	Medium	High	High

NEGATIVE CONSEQUENCES					LIKELIHOOD	POSITIVE CONSEQUENCES				
-5	-4	-3	-2	-1		1	2	3	4	5
E	E	H	H	M	ALMOST CERTAIN	M	H	H	E	E
E	E	H	M	M	LIKELY	M	M	H	E	E
E	H	M	M	L	POSSIBLE	L	M	M	H	E
H	H	M	L	L	UNLIKELY	L	L	M	H	H
H	M	L	L	L	RARE	L	L	L	M	H

where

-5 Catastrophic
 -4 Major
 -3 Moderate
 -2 Minor
 -1 Insignificant

E Extreme
 H High
 M Medium
 L Low

+1 Insignificant
 +2 Minor
 +3 Moderate
 +4 Major
 +5 Outstanding

Figure 24: Risk/Opportunity Matrix (from [50])

Risk Evaluation

Risk evaluation is based on the outcomes of the risk analysis, and its purpose is to decide whether a risk needs treatment, whether something needs to be done at all and according to what priorities. At this step of the risk management process the level of risk is compared with the pre-determined risk criteria within the established risk management contexts. Decisions are usually based on the level of risk or, in some cases, on thresholds in terms of specified consequences, likelihood of specified outcomes, cumulative effect of multiple events or range of uncertainty about the risk levels. Risk evaluation results in a ranked list of risks, prioritised for treatment. The risk evaluation has to consider the big picture including the stakeholders' objectives and risk tolerability, the degree of control over each risk, the cost, the benefits and potential opportunities. Moreover, decisions have to take into account the tolerability of the risks borne by parties other than the organisation that may benefit from them.

HB 436:2004 [49] provides a diagram introducing the 'as low as reasonably practicable' (ALARP) principle (reproduced in Figure 25). AS/NZS 4360:2004 does not even mention this descriptive risk evaluation tool. The area between the two levels: the basic safety limit and the basic safety objective, where costs and benefits are traded off in the risk evaluation process, is the ALARP region. Risks below the ALARP region are negligible or so small that no treatment is required, while risks above the ALARP region are so intolerable that treatment measures are essential irrespective of their potential benefits or risk treatment costs.

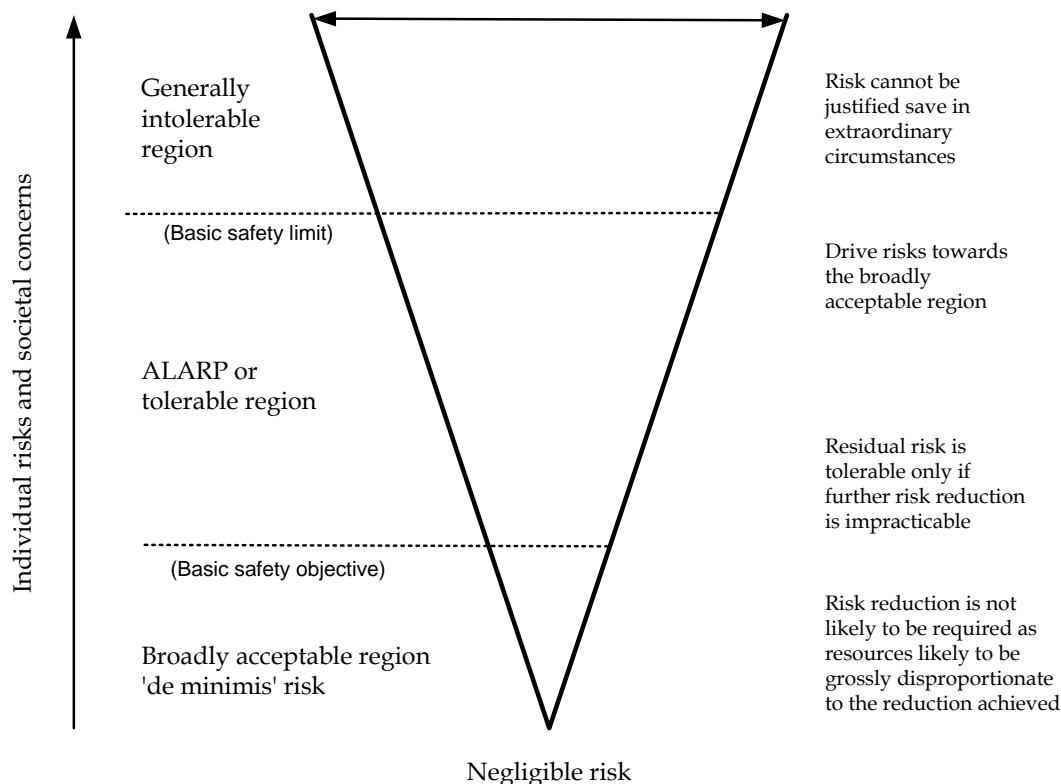


Figure 25: ALARP Principle (from [49])

ALARP as a principle appears to contain the idea of practicality, i.e. whether can be done, together with a cost-benefit estimate based on the question whether it is worth doing something in the given circumstances. When the risk is close to intolerable, risk treatment will be undertaken unless the treatment cost far exceeds the potential benefits. Where the risk is close to negligible, risk treatment may be undertaken only if the benefits clearly exceed the treatment cost.

The evaluation step of the risk management process ends with accepting, monitoring and reviewing risks of the lowest priority. All other unacceptable and prioritised risks are referred to the next risk treatment step.

Risk Treatment

Risk treatment consists of identifying treatment options for risks with positive and negative outcomes, assessing risk treatment options, preparing and implementing risk treatment plans and then,, making decisions about the residual risks. All activities have to meet the organisation's goals and objectives and be carried out within established funding limits. Moreover, the risk treatment resources should have been established at the context step of the risk management process.

For the risks with positive outcomes (opportunities) *treatment options have to be identified and considered, including:*

- Pursue the opportunity by proceeding with the risk containing activity where this is practicable. If the pursuit is inappropriately adopted without due consideration, it may compromise other potential opportunities or result in unnecessary risks. Alternatively, aversion to pursuing opportunities may lead to bad decision-making, delays in the treatment process, and/or, ultimately, failure to acknowledge the opportunities.
- Change the opportunity by increasing the likelihood of occurrence of the positive outcomes or changing the consequences to enhance the extent of the gains, or both. There is a trade-off between opportunity level and the cost to change an opportunity to an acceptable level. A priori formulated criteria have to form the basis of this optimisation procedure, while the specific circumstances and the established context will determine the most suitable criterion. Together, they will yield the solution to this opportunity enhancement problem.
- Share the opportunity by involving another organisation or organisations in whole or part of the opportunity. In this way the original organisation transfers some of its opportunity, for example using partnerships or joint ventures. However, new risks may emerge in the process as the recipient organisation(s) may not be able to manage the new opportunity appropriately. There is also some financial cost involved, when sharing an opportunity.
- Retain the opportunity, usually residual, after the completion of changing or sharing procedures. An opportunity may be retained by default when the organisation has not undertaken any action in treating it.

For the risks with negative outcomes various *treatment options have to be identified* and considered, including:

- Avoid the risk by not proceeding with the risk containing activity where this is practicable. If risk avoidance is inappropriately adopted due to a risk aversion attitude, it may cause an increase in the levels of other risks. Risk aversion may lead to bad decision making, delays in the risk treatment process, and ultimately failure to treat risk.
- Change the risk by decreasing the likelihood of occurrence of the negative outcomes or changing the risk consequences to reduce the extent of the losses, or both. There is a trade off between risk level and the cost of risk change to an acceptable level. A priori formulated risk criteria have to form the basis of this optimisation procedure while the specific circumstances and the established risk context will determine the most suitable criterion. Together, they will yield the solution to the risk reduction problem.
- Share the risk by involving another organisation or organisations in whole or part of the risk. In this way the original organisation transfers some of its risk, preferably by mutual consent. The overall risk level to society may not decrease and the recipient organisation may not manage its new risk appropriately. There is some financial benefit or cost, such as a premium paid for insurance, when sharing a risk.
- Retain the risk, usually residual, after the completion of risk reduction or risk transfer procedures. Risk may be retained by default when it is not treated by the organisation accordingly.

Note that the treatment options for risks with positive and negative outcomes are similar in concept, but the interpretation and implications are quite different; for details refer to Section 8 of HB 436:2004 [49].

To assess treatment options is to consider their feasibility, benefits and cost, to recommend treatment strategies, and to select a treatment strategy. Assessing treatment options is a process, which has to be conducted, with respect to the extent of risk/opportunity level reduction/enhancement, of the number of newly created risks/opportunities, of the size of the additional benefits/losses and with respect to the evaluation criteria including budget constraints. Usually a single treatment option cannot be the solution for a specific problem. A number of options have to be considered and applied together in combination as a treatment measure. For example, reduction of risk likelihood, reduction of risk consequences, risk sharing, and risk retention, if applied simultaneously may provide a better solution.

When assessing treatment options one has to base the decision making on balancing between an option's cost implementation and the benefits obtained from it. As a rule the cost has to be lower or at most commensurate with the benefits. Exceptions of this rule are risks of rare likelihood but catastrophic (severe) consequences. Such risks have to be treated despite potential or even real danger of being identified as unjustified in financial context. Further, if a high-level risk undertaking could be identified as having a considerable number of new opportunities emerging from it, then the assessment would have to include risk treatment cost and the risk consequences rectification cost. These two costs have to be weighed against the impact of the aforementioned opportunities. In general, the ALARP principle has to form the basis of the approach to dealing with the adverse risks.

Assessing treatment options may include implementation prioritising due to limited financial resources. Sometimes the cumulative cost of the options exceeds the budgeted one. Thus various techniques have to be applied to strictly determine the priority order under which the treatment options will enter the treatment plan.

Preparing and implementing treatment plans marks the next stage of the treatment step. Treatment plans show how the selected treatment measures have to be implemented. They have to clearly delegate responsibilities, provide time schedules, describe the expected treatment effects, secure adequate budgeting, determine performance measures, and establish a rigorous review process. Plans have to include performance criteria against which the implementation of the treatment options is to be tested. Treatment plans usually contain critical milestones needed in the implementation monitoring. Implementing treatment plans requires the existence of a management system capable of identifying the techniques to be used, assigning the responsibilities and accountabilities up to individual level, and monitoring the process against specified criteria.

Monitor and Review

Monitor and review is not just a step, but an ongoing process embedded in the risk management process. It deals with the performance of the risk management system and the potential changes affecting it according to AS/NZS 4360:2004 [36]. Risks change with time and circumstances. Hence the need to monitor them and their environments, the implementation of risk treatment plans, the system set up to control the risks and the established contexts and risk priorities. Review is a continuous process and an integral part of the risk management plan. It ensures that the plan stays relevant and up-to-date. It introduces all changes in the risk management process. The inevitable regular repetition of the risk management cycle is based on the review process.

Record the risk management process

Documentation has to be generated at each step of the risk management process. It will contain results, plans, reviews, assumptions, methods, data, etc. HB 436:2004 [49] prescribes appropriate documentation as required for the proper management of risk. Generally, documentation provides evidence of a systematic approach applied to the risk management process, helps flow of communication, provides the basis for accountability and auditing, facilitates any monitor and/or review process, establishes a solid background for decision making, helps develop archives and databases, etc. Section 10 of HB 436:2004 contains guidance on the appropriate documentation including examples.

DISTRIBUTION LIST

A Review of the Capability Options Development and Analysis System and the Role of Risk Management

Svetoslav Gaidow, Seng Boey and Richard Egudo

AUSTRALIA

DEFENCE ORGANISATION

	No. of copies
Task Sponsor	
COMD LWDC	1 printed
S&T Program	
Chief Defence Scientist	email pdf
Deputy Chief Defence Scientist Policy	email pdf
AS Science Corporate Management	email pdf
Director General Science Policy Development	email pdf
Counsellor Defence Science, London	Doc Data Sheet
Counsellor Defence Science, Washington	Doc Data Sheet
Scientific Adviser to MRDC, Thailand	Doc Data Sheet
Scientific Adviser Joint	email pdf
Navy Scientific Adviser	Doc Data Sht & Dist List
Scientific Adviser - Army	1 printed
Air Force Scientific Adviser	Doc Data Sht & Dist List
Scientific Adviser to the DMO	email pdf
Chief of Land Operations Division	Doc Data Sht & Dist List
Research Leader Human Systems Integration	1 printed
Research Leader Land Systems	1 printed
Research Leader Operations Research	1 printed
HTFM (Dean Bowley)	1 printed
HLFS (Darryn Reid)	
Authors:	
Svetoslav Gaidow	1 printed
Richard Egudo	1 printed
Chief of Air Operations Division	Doc Data Sht & Dist List
Seng Boey	1 printed
Chief of Maritime Operations Division	Doc Data Sht & Dist List
Chief of Defence Systems Analysis Division	Doc Data Sht & Dist List
OR Hub website (via EO, S&T Hubs, Stephen Mills)	1 pdf
DSTO Library and Archives	
Library Fishermans Bend	Doc Data Sheet
Library Edinburgh	2 printed

Capability Development Group

Director General Maritime Development	Doc Data Sheet
Director General Land Development	email pdf
Director General Capability and Plans	Doc Data Sheet
Assistant Secretary Investment Analysis	Doc Data Sheet
Director Capability Plans and Programming	Doc Data Sheet
Director General Australian Defence Simulation Office	Doc Data Sheet

Chief Information Officer Group

Director General Australian Defence Simulation Office	Doc Data Sheet
AS Information Strategies and Futures	Doc Data Sheet
Director General Information Services	Doc Data Sheet

Strategy Group

Assistant Secretary Strategic Planning	Doc Data Sheet
Assistant Secretary International and Domestic Security Policy	Doc Data Sheet

Navy

Director General Navy Capability, Performance and Plans, Navy Headquarters	Doc Data Sheet
Director General Navy Strategic Policy and Futures, Navy Headquarters	Doc Data Sheet
Maritime Operational Analysis Centre, Building 89/90 Garden Island Sydney NSW	
Deputy Director (Operations)	
Deputy Director (Analysis)	shared Doc Data Sht & Dist List

Army

J86 (TCS GROUP), DJFHQ	email Doc Data Sheet
ABCA National Standardisation Officer, Land Warfare Development Sector, Puckapunyal	e-mailed Doc Data Sheet
SO (Science) - Land Headquarters (LHQ), Victoria Barracks NSW	Doc Data & Exec Summ
SO (Science), Deployable Joint Force Headquarters (DJFHQ) (L), Enoggera QLD	Doc Data Sheet

Air Force

SO (Science) - Headquarters Air Combat Group, RAAF Base, Williamtown NSW 2314	Doc Data Sht & Exec Summ
---	--------------------------

Joint Operations Command

Director General Joint Operations	Doc Data Sheet
Chief of Staff Headquarters Joint Operations Command	Doc Data Sheet
Commandant ADF Warfare Centre	Doc Data Sheet
Director General Strategic Logistics	Doc Data Sheet

Intelligence and Security Group

Assistant Secretary Concepts, Capability and Resources	email pdf
DGSTA DIO	email pdf
Manager, Information Centre, DIO	email pdf

Director Advanced Capabilities, DIGO	Doc Data Sheet
Defence Materiel Organisation	
Deputy CEO	Doc Data Sheet
Head Aerospace Systems Division	Doc Data Sheet
Head Maritime Systems Division	Doc Data Sheet
Chief Joint Logistics Command	Doc Data Sheet
Program Manager Air Warfare Destroyer	Doc Data Sheet
Guided Weapon and Explosive Ordnance Branch	email Doc Data Sheet
OTHER ORGANISATIONS	
National Library of Australia	email pdf
NASA (Canberra)	email pdf
UNIVERSITIES AND COLLEGES	
Australian Defence Force Academy	
Library	email pdf
Head of Aerospace and Mechanical Engineering	email pdf
Hargrave Library, Monash University	Doc Data Sheet
OUTSIDE AUSTRALIA	
INTERNATIONAL DEFENCE INFORMATION CENTRES	
US Defense Technical Information Center	email pdf
United Kingdom - Dstl Knowledge Services	email pdf
Canada - Defence Research Directorate R&D Knowledge & Information Management (DRDKIM)	email pdf
NZ Defence Information Centre	email pdf
ABSTRACTING AND INFORMATION ORGANISATIONS	
Library, Chemical Abstracts Reference Service	email pdf
Engineering Societies Library, US	email pdf
Materials Information, Cambridge Scientific Abstracts, US	email pdf
Documents Librarian, The Center for Research Libraries, US	email pdf
SPARES	5 printed
Number of copies:	
Printed	16
PDF	23
Total	39

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION DOCUMENT CONTROL DATA					
				1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)	
2. TITLE A Review of the Capability Options Development and Analysis System and the Role of Risk Management			3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION) <div style="display: flex; justify-content: space-between;"> Document (U) </div> <div style="display: flex; justify-content: space-between;"> Title (U) </div> <div style="display: flex; justify-content: space-between;"> Abstract (U) </div>		
4. AUTHORS Svetoslav Gaidow, Seng Boey and Richard Egudo			5. CORPORATE AUTHOR Defence Science and Technology Organisation PO Box 1500 Edinburgh South Australia 5111 Australia		
6a. DSTO NUMBER DSTO-GD-0473		6b. AR NUMBER AR 013-727		7. DOCUMENT DATE August 2006	
8. FILE NUMBER 2005/1014084		9. TASK NUMBERS ARM 02/079 ARM 02/080		10. TASK SPONSOR COMD LWDC	
				11. NO. OF PAGES 58	
				12. NO. OF REFERENCES 50	
13. URL on the World Wide Web http://www.dsto.defence.gov.au/corporate/reports/DSTO-GD-0473.pdf				14. RELEASE AUTHORITY Chief, Land Operations Division	
15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT <div style="text-align: center;"><i>Approved for public release</i></div>					
OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111					
16. DELIBERATE ANNOUNCEMENT No limitations					
17. CITATION IN OTHER DOCUMENTS				Yes	
18. DSTO Research Library Thesaurus Capability development Risk management					
19. ABSTRACT Capability development is a complex process that requires significant science & technology support and a rigorous analytical background. In the Australian Army, this need has led to the design of the Capability Options Development and Analysis System (CODAS) at the Force Development Group of the Land Warfare Development Centre. This document contributes towards analysis of CODAS as a system, the evolution of its architecture and its role as an analytical support framework for capability development in the Army. It also aims to reveal the potential of risk management as a valuable analysis and decision-making support tool belonging to CODAS. The application of risk management in capability development can be viewed as realisation of the CODAS methodology and thus raises the profile of CODAS in the Army Continuous Modernisation Process.					